From: "Barrett, Michael" <mbarrett@paypal.com>
To: <DNSSEC@ntia.doc.gov>
Date: Fri, Nov 21, 2008 10:14 PM
Subject: Re: Notice of Inquiry on Enhancing the Security and Stability of the Internet's Domain Names and Addressing System - 73 Fed. Reg. 59608 (Oct. 9, 2008)

TO: DNSSEC@ntia.doc.gov

FROM: Michael Barrett, Chief Information Security Officer, PayPal

RE: Notice of Inquiry on Enhancing the Security and Stability of the Internet's

Domain Names and Addressing System - 73 Fed. Reg. 59608 (Oct. 9, 2008) and
http://www.ntia.doc.gov/frnotices/2008/FR_DNSSEC_081009.pdf

DATE: November 21, 2008

Thank you for this opportunity to comment on implementation of DNSSEC (Domain Name and Addressing System Security Extensions) at the root zone level, on behalf of PayPal. Since 1998, PayPal has been the global leader in online payment solutions. While PayPal has only been in business a decade, it has about 165 million users globally, operates in 190 markets, and settles in 19 major currencies; in 2007 we processed over $47 billion in payments.

As a major online financial services institution, the safe and secure operation of the Internet is of vital importance to PayPal's business. This safety and security, and indeed the ongoing viability of electronic commerce, depend on the trust of consumers. They must know that they are interacting with the real PayPal and not a phishing site. PayPal has been a leader in the deployment of technologies that enable this trust. PayPal was one of the first deployers of EV (Extended Validation) SSL (Secure Sockets Layer) digital certificates. It applies digital signatures to all email it sends to consumers. These techniques enable consumers, ISPs, and software clients to make trust decisions about what content is legitimately from PayPal. However, there are limits to what any single company can do to make the Internet experience of our customers safe and secure. The current weakest link in the trust

chain on the Internet is the DNS (Domain Name System).

In this context, the rapid adoption of DNSSEC (DNS Security Extensions) and signing of the root zone is an urgent requirement. We applaud NTIA for initiating this inquiry, and urge it to move with all possible speed to implement DNSSEC. Inaction or further delay would be detrimental to the interests of consumers and other Internet users, and to the healthy growth of electronic commerce.

Background

We believe that there are three major threats to the internet user that are related to authentication or identifying who users are communicating with:

1. Spoofed websites

2. Spoofed Email

3. Spoofed DNS

The first two threats are being managed. SSL, along with EV certificates, largely solves the general problem of spoofed websites from a technology standpoint - at least for those sites that can put all of their traffic across SSL. Email signing via DKIM (Domain Keys Identified Mail) along with other technologies such as ADSP (Author Domain Signing Practices), and reputation services, mostly solve the problem of spoofed email. This leaves DNS spoofing as the main unaddressed vulnerability in this sphere. DNSSEC is the best available tool for addressing this threat.

DNS spoofing currently falls into two categories, both of which we believe are threats to PayPal, to our customers, and to consumers and Internet users in general. The first type of spoofing is done by an attacker. These attacks can occur on public networks such as a public wireless access point, or they can be targeted against DNS infrastructure at the ISP. With the vulnerabilities inherent in the DNS protocol's UDP delivery mechanism and lack of strong encryption for transport, DNSSEC represents the only way for a consumer and an ISP to identify a legitimate DNS response.

The second threat of DNS spoofing comes from DNS infrastructure operators themselves. Many DNS providers, registries, and ISPs are performing DNS spoofing as a way to monetize user errors, such as when a user attempts to access a domain name that does not exist. In the case of DNS spoofing of non-existent domains we believe this is an internet governance problem between ICANN and the registry for a given TLD.

A more insidious type of DNS spoofing has taken hold lately that we believe is also a threat. This is the spoofing of DNS responses for non-existent sub-domains of legitimate domains within DNS. Many ISPs in the US and elsewhere are spoofing DNS replies for DNS requests that generate an NXDOMAIN record type from the SOA (Start of Authority) for that domain. For example, when a user mistypes ww.paypal.com (intending to type www.paypal.com), the ISP will serve that user a spoofed DNS reply that points the user at an ad server run by the ISP. This ISP ad server will receive cookies intended for the domain in question, can set cookies for the domain in question, and is now within the security perimeter of the domain owner without the owner's permission. As a result, security features within the intended site may no longer work properly, and the consumer's security is jeopardized. In the worst-case scenario, bad actors could use this technique to generate a spoofed reply pointing to a fake site intended to mimic the actual PayPal site. Consumers using an ordinary internet connection have no mechanism for determining that this response was spoofed. DNSSEC is currently the only security technology that would reveal to the typical consumer that the response was spoofed, and allow the consumer to make an informed choice about this illegitimate behavior by the ISP.

The Value of DNSSEC

DNSSEC and root zone signing solve several critical security problems and provide the basis for new developments in the secure delivery of information, such as signed security policies, secure SPF policy delivery, and the secure delivery of information such as that contained in DNS SRV records. No other alternative for providing the secure delivery of this information is on the horizon. Kaminsky's work on exposing new exploits against previously known structural weaknesses in the DNS protocols has increased the pressure and need for DNS authentication. While theoretically, there might be better technical solutions than DNSSEC, we do not believe that there is enough time to contemplate development of an alternative protocol to DNSSEC, which currently represents the only viable option for the secure delivery of this type of information.

The main hurdles to overcome are those related to responsibility and authority for management of the root zone signing keys and the signing itself. In this matter we believe there are short term and long term considerations.

In the short term we believe that getting the root zone signed, even under the auspices of a single root signing authority, is preferable to waiting for consensus to emerge about per-country or M-of-N signature proposals. While we recognize that single authority systems may not be as robust in the face of certain types of attacks, and could be vulnerable to political pressure, we believe that these issues should be decoupled from the implementation timeframe for initial signing of the root zone. A single authority should sign the root zone as soon as possible. We believe that there is now limited time before usable brute force attacks are available to criminals, and therefore rapid deployment of DNSSEC is the only viable solution.

Based on currently submitted proposals we believe that IANA or ICANN should be given the authority and responsibility for implementing the initial root zone signing. Of the choices presented in the Notice of Inquiry, Proposed Process Flow #4 would accomplish this, though there are other options for achieving this result. Given the current role of ICANN in governance, and of IANA (as administered by ICANN) in root zone maintenance, this would be the natural choice for the authority and responsibility for root zone signing. However, we do have operational concerns related to security practices of whoever is chosen. On this issue, we urge NTIA to seek expert guidance from organizations (such as root Certification Authorities) that have experience in handling the type of sensitive materials involved in these operations.

Longer term, we believe that some form of M-of-N or simple multiple signing authorities approaches should be explored. Vesting control of root zone signing in one entity is too tempting an attack target and too subject to political pressure from a single government or entity. Ultimately end-user and DNS infrastructure software will be the main consumers of DNSSEC data. Just like the current situation in web browsers, where a list of Root CA Certificates is deployed, we expect a similar model will be necessary for DNSSEC. Given the already existing software infrastructure and ecosystem for allowing multiple Root CA certificates in end-user software, we believe M-of-N, or at the very least multiple signatures on the root zone or other TLDs, is in practice workable. We recommend that this option be further developed, but we do not think it would be prudent to wait until it is fully developed before signing the root using DNSSEC.

Finally, I would like to publicly recognize the significant contribution of Andy Steingruebl, Principal Information Security Engineer in the PayPal Information Security team, in helping form our opinion. He facilitated my team in coming to a consensus on this difficult issue, and performed extensive analysis of the various options presented in the Notice of Inquiry.

PayPal appreciates the opportunity to provide comments. We would be glad to provide further information on this topic and look forward to working with NTIA in closing the existing vulnerabilities of the DNS through prompt adoption of DNSSEC.

Respectfully submitted,

Michael Barrett

Chief Information Security Officer, PayPal