Securing a Domain: SSL vs. DNSSEC

By Howard Eland
Senior Director Of Content Propagation and Resolution , Afilias

There has been quite a bit of talk lately about the best way to secure a domain, mainly centered in two camps: using Secure Socket Layer (SSL), or using DNS Security Extensions (DNSSEC). The answer is quite simple – you should use both.

The reason for this is that they solve different problems, using different methods, and operate over different data. This is analogous to having an electronic security system and a very large dog. Both protect the house, but they do it in radically different ways (very few burglars have been bitten by a surveillance system). To better understand this, we need to examine how each system works, what it does, and, more specifically, what it doesn't do.

Secure Socket Layer, or SSL, is a system used to encrypt data and authenticate the sender (in this case, the sender is the website you're connecting to). To facilitate the encryption, the folks running the web site must obtain what's known as an SSL Certificate. Think of it like a birth certificate: it says “yes, this website is who they claim to be”. This certificate contains a public and a private electronic key, which is used to establish a secure channel (called a session) between your browser and the web site. With the session established, all data passing between the website and your browser is encrypted – to anyone snooping around on the network, looking at your packets, it appears garbled.

DNS Security Extensions (DNSSEC) doesn't work with websites at all – it's all done behind the scenes, before any web-stuff occurs. When a home computer uses DNSSEC to try to find a web site's address, it not only performs the normal DNS lookup, it also validates a signature returned from the DNS server. This happens at all levels, from the “root servers”, through the Top Level Domain (e.g. .org or .info) all the way down to the specific address that you requested (www.example.org). If all of these signatures are validated, then the answer is sent to the browser to connect to the web site (and maybe using SSL to do so).

So why not just use one or the other? Let's start with just using SSL. Remember the birth certificate analogy? The certificates come from establishments known as Certificate Authorities, or CAs (this is the “hospital”). The problem is that some CAs are not trustworthy, and will issue certificates without checking any data on the company itself. This means that anyone could, using the right CA, be issued a certificate for www.example.org. It is also possible for people to “self-sign” a certificate – in effect, becoming their own hospital. Many phishing sites do this now, and make their certificate look as legitimate as possible.

Using just DNSSEC isn't fool proof either. Even though you have completely determined that the "chain of trust" has been followed all the way down from the root DNS servers, you now have to transmit sensitive data to a Web site (such as your bank account login and password).   DNSSEC does not do any data encryption on the DNS, and isn't involved at all once the web interaction has started. This means that anyone watching your network (which, on WiFi, is very easy to do these days) could easily steal your information.

So, in conclusion, using DNSSEC and SSL is not simply a "belt and suspenders" rule – it's more of a "shirt and pants" rule. Using either is good, but using both will increase your security significantly, causing the least, um, exposure.