DNCSEC

Secure DNS or DNSSEC

Some common attacks include DNS Hijacking, DNS Poisoning, and Man-in-the-Middle attacks. Most of the DNS attacks exploit unsecured DNS protocol which allows threat actors to impersonate other's by changing name resolution. DNS attacks are especially dangerous because they are easily exacerbated by the normal internet practices of normal users. DNSSEC (DNS Security Extensions) uses digital signatures on data to ensure integrity. Hierarchical digital signitures are present at all layers of the DNS protocol in DNSSEC. DNSSEC is backwards compatible, such that traditional, non-secure DNS lookups still resolve correctly. DNSSEC requires TLS or SSL.

Additionally, DNS Server redundancy, A.K.A. Anycast Routing or Load Balancing can prevent DNS-based DDoS attacks. DNS Firewalls, from companies like Cloudflare and UpCloud.

CloudFlare touts the lowest DNS query speed, as well as the fastest DNS propagation.

CloudFlare’s DNSSEC adds an authentication layer to DNS, and guarantees that querists reach the website they intended to, supplanting Man-in-the-middle attacks and DNS poisoning. DNS is fundamentally insecure and this service secures the infrastructure. CloudFare uses zone enumeration, in addition to certificate infrastructure, to ensure DNS integrity.

According to Rob and Ryan, most of our client’s registrars are GoDaddy or NameCheap. GoDaddy and NameCheap will work with CloudFlare’s DNSSEC. Network Solutions will likely work as well but there is less certain documentation on that. Using CloudFlare’s DNS services with a different registrar requires that the CloudFlare admin finds the DS Record from CloudFlare’s control panel, and manually add that to the registrar control panel. The following guide features a table that illustrates the procedure for each of the most popular registrars: <https://support.cloudflare.com/hc/en-us/articles/360006660072#nodnssec>

CloudFlare uses a dashboard/control panel over HTTPS. Their preferred encryption cipher is the asymmetric Algorithm 13, which features elliptical curve (low processing requirements) cryptography, zone signing, and signatures. This is the same protocol that is used by Bitcoin to ensure confidentiality, integrity, and non-repudiation.

According to DNSSECready.net, https://sets.solar will be fine to implement DNSSEC since the .solar top-level domain (TLD) is signed and validated. This will definitely prohibit any domain with more unusual TLDs like .vi or .tel. I could think of no other clients that has non-standard TLDs.

DNSSEC adds additional record types, including RRSIG, DNSKEY, DS, NSEC(3), CDS or CDNSKEY. The most important of these for troubleshooting purposed will be the DS record, which contains a hash of the DNSKEY record and must be manually added to registrar’s records. DNSSEC also creates RRsets, which are collections of records with the same type (A, CNAME, MX, etc.), that are grouped into resource record sets, which are then digitally signed.

Whenever a DNSSEC resolver requests a particular record type (like AAAA), the name server will return the record in addition to a corresponding RSIG record, which contains a cryptographical digital signature.

DNSSEC is to DNS what HTTPS is to the internet. DNSSEC adds additional layers of security by authenticating and signing. DNSSEC does not *encrypt* DNS queries, unlike HTTPS. Instead it offers digital signatures so that MITM and DNS-poisoning attacks, and forgeries, redirects, and even DNS-hijacking are no longer threats.

Implementing CloudFlare DNSSEC is pretty straightforward. Once the service is started, DNSSEC can be added to any web property by enabling DNSSEC there and adding the DS record to the registrar. Going forward, it is also possible to use CloudFlare as a registrar, where DNSSEC is included.

I have enrolled for the free version of DNSSEC through CloudFlare, and it begins with entering the site you own, then allowing CloudFlare to query your site’s existing DNS records, and import them into CloudFlare’s database. Then the name servers will need to be changed to CloudFlare, where they tout a <5m DNS propagation. The free version I selected includes global content delivery network (CDN) which provides cached content, high availability, increased security against DDoS’s. It also includes SSL certificates. The Business model is $200 per month, and includes Web Application Firewalls with custom CloudFlare rulesets, TLS-only-mode, custom SSL certificates, and image/mobile-browser optimizations. The Enterprise level required a call to determine pricing, and features the best support, access to raw request logs, and 100% uptime guarantee with a very generous reimbursement for SLA violations.

CloudFlare’s auto lookup got every record for my grandmother’s website, <https://www.horwitzstudio.com>, hosted on WordPress. Despite WordPress’s assertion that using non-WordPress nameservers would cause “some WordPress features to fail to load”, I saw no impact in performance or availability. WordPress isn’t known for being the most lightweight and adaptable service, and even still it seemed to work fine.

The <5m propogation was nullified by the admission that it may take up to 24 hours for the registrar to publish the changes. At 12:15pm on Thursday the 9th, I made the change, and I ran a constant ping on my Linux machine (at home) to see if the IP address change was detectable. I wrote a short recursive script that runs a traceroute every 30 seconds and pipes the output into a text file. The script and the output of that text file are available on my Github: https://github.com/bcornw2/