F5 Technical Brief

DNSSEC: The Antidote to DNS Cache Poisoning and Other DNS Attacks

Domain Name System (DNS) provides one of the most basic but critical functions on the Internet. If DNS isn't working, then your business likely isn't either. Secure your business and web presence with Domain Name System Security Extensions (DNSSEC).

by Peter Silva
Technical Marketing Manager

With contributions from
Nathan Meyer, Product Manager
Michael Falkenrath, Senior Field Systems Engineer

Contents

Introduction

Humans have always had difficulty remembering number sequences. Back in 1956, George Miller did some research on digit span recall tasks and found that humans are only able to hold seven plus or minus two items in memory.[1] He concluded that even when more information is offered, the human memory system has the capacity to remember between five and nine chunks of information. Most people have a vocabulary of 10,000 to 30,000 words and some suggest that 500 to 1,000 of those are names. We've experienced words in place of numbers for years with the telephone system, especially 800 numbers, when a company spells out its product, name, or industry—like 1-800-EAT-SOUP.

It should come as no surprise that when the Internet was invented with all its numbered Internet Protocol addresses, humans needed a way to translate those numbers into understandable names. The Domain Name System (DNS) was created in 1983 to enable humans to identify all the computers, services, and resources connected to the Internet by name. DNS translates human readable names into the unique binary information of devices so Internet users are able to find the machines they need. Think of it as the Internet's phone book.

Now what would happen if someone changed your business name and matching phone book entry to his or her own? The phone book now lists "A. Crook," an imposter who receives all of your calls and controls your number. Or, what if someone completely deleted your entry and no one could find you? That would really hurt business. What if that same situation happened to the domain name tied to your public website? An e-commerce site, at that! Either your customers won't be able to find you at all or they will be redirected to another site that might look exactly like yours, but it is really A. Crook's site. A. Crook happily takes their orders and money, leaving you with lost revenue, downtime, or any of the other myriad of issues organizations face when their web property is hijacked.

Security was not included in the original DNS design since at the time scalability—rather than malicious behavior—was the primary concern. Many feel that securing DNS would go a long way to securing the Internet at large. Domain Name System Security Extensions (DNSSEC) attempts to add security to DNS while maintaining the backward compatibility needed to scale with the Internet as a whole. In essence, DNSSEC adds a digital signature to ensure the authenticity of certain types of DNS transactions and, therefore, the integrity of the information.

DNSSEC provides:

- Origin authentication of DNS data.
- Data integrity.
- Authenticated denial of existence.

Challenges

DNS in the Wild: Bad Things Can Happen

DNS has worked just great since its inception, but as with almost everything Internet-related, the bad guys have found ways to exploit the protocol. One such way is called DNS cache poisoning. When you type a URL into your browser, a DNS resolver checks the Internet for the proper name/number translation and location. Typically, DNS will accept the first response or answer without question and send you to that site. It will also cache that information for a period of time until it expires, so upon the next request for that name/number, the site is immediately delivered. DNS won't need to query the Internet again and uses that address until that entry expires. Since users assume they are getting the correct information, it can get ugly when a malicious system responds to the DNS query first with modified, false information, as it does with DNS cache poisoning. The DNS servers first send the user to the bad link but also cache that fake address until it expires. Not only does that single computer get sent to the wrong place, but if the malicious server is answering for a service provider, then thousands of users can get sent to a rogue system. This can last for hours to days, depending on how long the server stores the information, and all the other DNS servers that propagate the information can also be affected. The imminent dangers posed by a rogue site include delivering malware, committing fraud, and stealing personal or sensitive information.

In 2009, the main DNS registrar in Puerto Rico was hacked by a DNS attack.[2] Local versions of the websites for Google, Microsoft, Coca-Cola, Yahoo, and others such as PayPal, Nike, and Dell were redirected to defaced sites or blank pages that told users that the requested site had been hacked. In this instance, the users were aware that they were not visiting the real site since the group who claimed responsibility gave notice. In a more sinister incident, one of Brazil's largest banks suffered an attack that redirected users to a malicious site that attempted to install malware and steal passwords.[3] In this situation, the users were not aware that they were on a fake site since the delivered page looked just like the original. These types of attacks are very hard to detect since the users had actually typed the correct domain name in their browsers.

Taming the Wild

DNSSEC is a series of DNS protocol extensions, defined in Request for Comments (RFCs) 4033, 4034, and 4035, that ensures the integrity of data returned by domain name lookups by incorporating a chain of trust into the DNS hierarchy. The chain is built using public key infrastructure (PKI), with each link in the chain consisting of a public/private key pair. DNSSEC does not encrypt or provide confidentiality of the data, but it does authenticate that data.

DNSSEC provides the following:

- **Origin authentication of DNS data:** Resolvers can verify that data has originated from authoritative sources.
- **Data integrity:** Resolvers can verify that responses are not modified in flight.
- **Authenticated denial of existence:** When there is no data for a query, authoritative servers can provide a response that proves no data exists.

Deploying DNSSEC involves signing zones with public/private key encryption and returning DNS responses with signatures. (See Figure 1.) A client's trust in those signatures is based on a chain of trust established across administrative boundaries, from parent to child zone, using a new DNSKEY and delegation signer (DS) resource records. Any DNSSEC deployment must manage cryptographic keys: multiple key generation, zone signing, key swapping, key rollover and timing, and recovery from compromised keys.

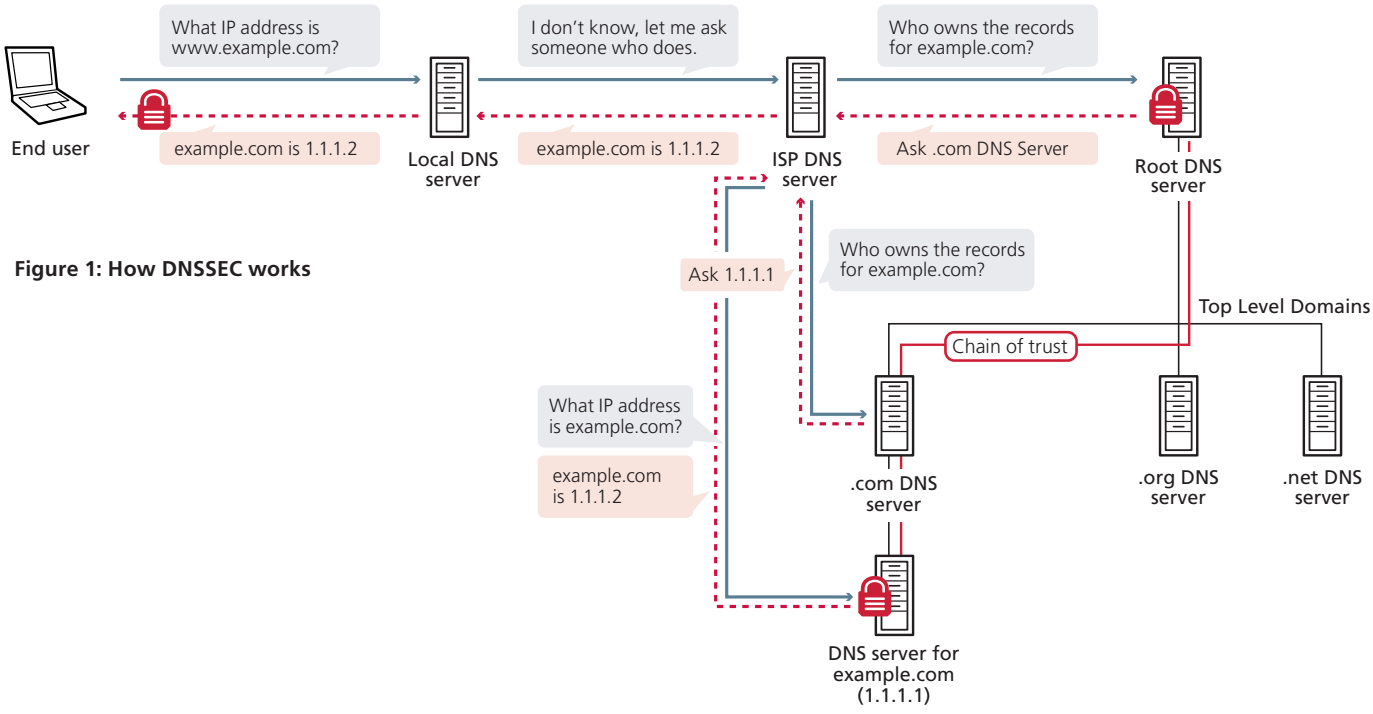

Figure 1: How DNSSEC works

To accomplish DNSSEC:

1. Each DNSSEC zone creates one or more pairs of public/private key(s) with the public portion put in DNSSEC record type DNSKEY.
2. The zones sign all resource record sets (RRsets) and define the order in which multiple records of the same type are returned with private key(s).
3. Resolvers use DNSKEY(s) to verify RRsets; each RRset also has a signature attached to it that is called RRSIG.

If a resolver has a zone's DNSKEY(s), it can verify that RRsets are intact by verifying their RRSIGs. The chain of trust is important to DNSSEC since an unbroken chain of trust needs to be established from the root at the top through the top-level domain (TLD) and down to individual registrants. All zones need to be authenticated by "signing," in that the publisher of a zone signs that zone prior to publication, and the parent of that zone publishes the keys of that zone. With many zones, it is likely that the signatures will expire before the DNS records are updated. Zone operators therefore require a means to automatically re-sign DNS records before these signatures expire. This functionality is called "continuous signing" or "automated key rollover" and is not yet a feature of common name server implementations.

Solutions

BIG-IP v10.1 and DNSSEC: The Keys to Success

F5® BIG-IP® v10.1 supports DNSSEC as an add-on feature to BIG-IP® Global Traffic Manager™ (available as a standalone device or as a module on BIG-IP® Local Traffic Manager™). BIG-IP Global Traffic Manager (GTM) is a global load balancer that provides high availability, maximum performance, and centralized management for applications running across multiple and globally dispersed data centers. BIG-IP GTM distributes end-user application requests according to business policies and data center and network conditions to ensure the highest possible availability. The BIG-IP GTM DNSSEC feature signs DNS responses in real time and provides the means to deploy DNSSEC quickly and easily in an existing environment.

If client requests a website that sits behind a BIG-IP device but does not request an authenticated answer, the BIG-IP GTM DNSSEC feature does nothing and BIG-IP GTM responds normally—passing through the BIG-IP device's virtual IP address to the DNS server pool and returning directly to the client. When authentication is

requested, the BIG-IP GTM DNSSEC feature intercepts the response and signs the response before sending it to the client computer. (See Figure 2.) In this instance, the DNSSEC request passes through BIG-IP GTM to the DNS servers. When the response is returned, BIG-IP GTM signs the response in real time to ensure continuous signing. The potential attacker cannot forge this response without the corresponding private key. The internal communication between BIG-IP GTM and the DNS server is normal and the external client communication is secure.

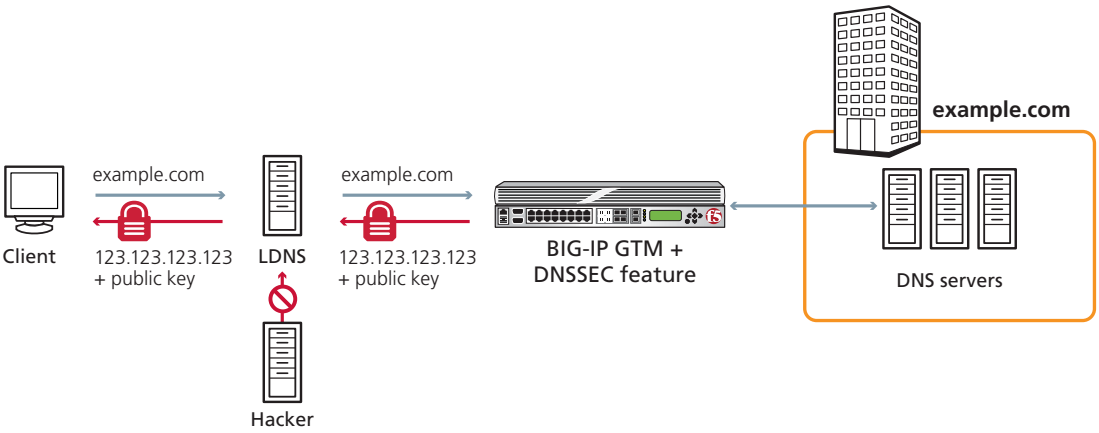

Figure 2: BIG-IP GTM DNSSEC feature interaction

This real-time signing is critical in dynamic content environments where both objects and users might be coming from various locations around the globe. There are other devices claiming DNSSEC for static DNS and DNSSEC compliance in general, but none of them has good solutions for dynamic content and none, so far, has any solutions for global server load balancing (GSLB)-type DNS responses in which the IP answer can change depending on the requesting client. Since GSLB can provide different answers to different clients for the same fully qualified domain name (FQDN), GSLB and DNSSEC are fundamentally at odds in the original design specifications. DNSSEC, as originally conceived, was focused solely on traditional static DNS and never considered the requirements of GSLB, or intelligent DNS. It's relatively easy to use BIND to provide DNSSEC for static DNS. It's more difficult to provide DNSSEC for dynamic DNS, and it's very difficult to provide DNSSEC for GSLB-type DNS responses, especially in cloud deployments. F5's general purpose DNSSEC feature provides DNSSEC covering all three scenarios and is simple to implement and maintain while keeping management costs low.

F5's unique, patent-pending solution to the GSLB DNSSEC problem addresses this by signing answers at the time the GSLB device decides what the answer should be.

This is a real-time DNSSEC solution, and, with it, F5 is the only GSLB provider to have a true DNSSEC solution that works. While others have proposed a system in which every possible response is pre-signed, most have concluded that this isn't a feasible approach.

Assuming BIG-IP GTM is already up, configured, and functioning—including DCs, servers, listeners, WIPS, and so on—the DNSSEC key list (see Figure 3) is where the administrator configures zone signing keys (ZSKs) and key signing keys (KSKs). KSKs are used to sign other DNSKEY records and the DS records, while ZSKs are used to sign RRSIG. It is best practice to name the keys with the zone name and either zsk or ksk at the end in order to easily identify them. The KSK can be made stronger by using more bits in the key material. It has little operational impact since it is only used to sign a small fraction of the zone data and to verify the zone's key set, not for other RRsets in the zone. The KSK should be rotated every 12 months and the ZSK every one to two months. No parent/child interaction is required when ZSKs are updated.

The BIG-IP GTM DNSSEC feature's default settings are modeled on the National Institute of Standards and Technology (NIST) guidelines, offering an easy, turnkey means to deploy this powerful solution.

Required options include:
Name
Algorithm
Bit width
FIPS
Type (zone signing keys)

Optional items include:
Rollover period
Expiration period

Note: The default is no automatic rollover

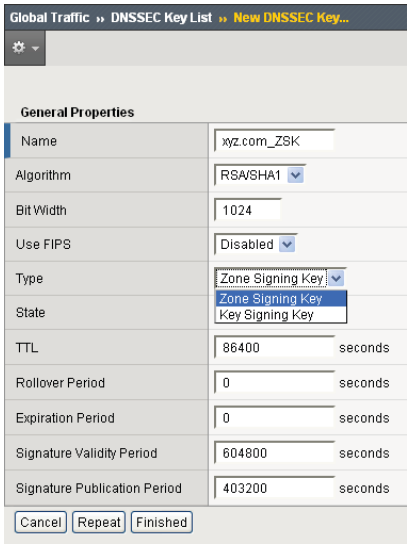

Figure 3: The GUI on the F5 BIG-IP system makes it simple to quickly configure and secure your DNS infrastructure.

Since the KSK is only used to sign a key set, which is most probably updated less frequently than other data in the zone, it can be stored separately from and in a safer location than the ZSK. A KSK can have a longer key effectivity period. For almost any method of key management and zone signing, the KSK is used less frequently than the ZSK. Once a key set is signed with the KSK, all the keys in the key set can be used as ZSKs. If a ZSK is compromised, it can be simply dropped from the key set and the new key set is then re-signed with the KSK.

If a KSK is to be rolled over, there will be interactions with parties other than the zone administrator. These can include the registry of the parent zone or administrators of verifying resolvers that have the particular key configured as secure entry points. Hence, the key effectivity period of these keys can and should be made much longer.

The public key enables a client to validate the integrity of something signed with the private key and the hashing enables the client to validate that the content was not tampered with. Since the private key of the public/private key pair could be used to impersonate a valid signer, it is critical to keep those keys secure. F5 employs two industry-leading techniques to accomplish this security task. First, for non-FIPS requirements, F5 employs Secure Vault, a super-secure SSL-encrypted storage system used by BIG-IP devices. Even if the hard disk was removed from the system and painstakingly searched, it would be nearly impossible to recover the contents of Secure Vault.

For military-level security, F5 supports FIPS storage of the private keys, and this is a unique differentiator from many of the DNSSEC providers on the market. Also unique to F5 is the ability to securely synchronize the keys between multiple FIPS devices. Additionally, multiple models of F5 hardware (BIG-IP 1500, 3400, 6400, 6800, 8400, and 8800) take a further step by using the crypto storage chip on the motherboard to secure a unique hardware key as part of the multi-layer encryption process.

When creating DNSSEC zones, use the most specific FQDN as its name. BIG-IP GTM will search the set of DNSSEC zones to find the most specific one to use when signing, even if multiple candidates exist.

(1) Name the DNSSEC zone.

(2) Choose the signing key.

(3) Choose the key signing key.

Conclusion

DNSSEC ensures that the answer you receive when asking for name resolution comes from a trusted name server. Since DNSSEC is still far from being globally deployed and many resolvers either haven't been updated or don't support DNSSEC, implementing the BIG-IP GTM DNSSEC feature can greatly enhance your DNS security right away. It can help you comply with federal DNSSEC mandates and help protect your valuable domain name and web properties from rogue servers sending invalid responses.

F5 BIG-IP v10.1 now provides DNSSEC signing for DNS records and real-time DNSSEC signing as requested by clients. The combination of BIG-IP Local Traffic Manager + BIG-IP GTM + DNSSEC on one box provides a drop-in DNSSEC solution for any existing DNS deployment, instantly giving you greater control and security over your DNS infrastructure while meeting U.S. Government mandates for DNSSEC compliance.

Rather than ripping and replacing your current DNS infrastructure, you can simply drop BIG-IP GTM in front of your existing DNS servers and reduce your management costs with implementation and maintenance all on the same appliance.

Resources

DNSSEC.net

DNSSEC Resource Center

National Institute of Standards and Technology

Tech Republic

Public Interest Registry

[1] Miller, G. A. (1956). The magical number seven plus or minus two: Some limitations on our capacity for processing information. Psychological Review, 63, 81-97.

[2] Puerto Rico sites redirected in DNS attack, CNET News, Apr. 27, 2009.

[3] Cache-poisoning attack snares top Brazilian bank, The Register, Apr. 22, 2009.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

CS10073 1109