Trusted Cyber Technology

THALES

Securing Infoblox DNSSEC Implementations with Thales TCT's Luna Network HSM

The Domain Name System (DNS) is the Internet's standard naming service, and is responsible for mapping domain names to IP addresses. Virtually all Internet applications rely on DNS. As the Internet has gained popularity, attacks on the DNS servers have become common. One category of these attacks, known as DNS spoofing or cache poisoning, seeks to divert users to malicious websites by corrupting a DNS name server's cache database. While most types of attacks against DNS can be dealt with by patching the name server software, some of these "cache poisoning" attacks are caused by inherent flaws in DNS. The only way to address these flaws is to introduce a layer of security on top of the DNS protocol.

DNSSEC Adds a Layer of Security to DNS

Domain Name System Security Extensions (DNSSEC) is a set of extensions added to DNS, providing a layer of security to mitigate the inherent vulnerabilities in the DNS protocol. DNSSEC is not a bottom-up redesign of the Internet's naming service, but rather is built on the "classic" Domain Name System, introducing new resource record types to DNS and extending the DNS message header. It is important to note that deploying DNSSEC will not break existing name servers or stub resolvers. This is critical since there are over 12 million name servers on the Internet and even more resolvers—upgrading them all will take a long time.

When DNSSEC is enabled on a zone, all resource record sets in the zone are digitally signed. By checking a record set's digital signature, a DNS resolver is able to validate that the records come from the authentic zone and have not been modified since they were signed. Note that DNSSEC does not provide confidentiality of data; in particular, all DNSSEC responses are authenticated but not encrypted. DNSSEC provides a security layer that supports the following use cases:

- Origin authentication—Ensures the data in the resource record set was created by the administrator of the DNS zone.
- Integrity checking—Ensures the data in the resource record set was not changed after it was created and signed by the administrator of the DNS zone.
- Ensures Chain of Trust—Ensures

DNSSEC and Asymmetric Cryptography

The digital signatures in DNSSEC are based on asymmetric cryptography, sometimes referred to as public-key cryptography. At the heart of asymmetric cryptography is the key pair, two mathematically-related cryptographic keys that have very special properties. In the most common scenario, one key is kept secret and used to encrypt data. This is called the private key. The other key is distributed and used to decrypt data that was encrypted with the private key. This is called the public key. Since the private key is a secret and not easily derivable from the public key, encrypted data that decrypts successfully using the public key is proven to have been encrypted, or "signed", by someone in possession of the private key.

This brings us to DNSSEC's main use cases—origin authentication and integrity checking. To add the security layer, each DNS zone is associated with one or more key pairs. The private key is held by the zone's administrator and kept secret. The signatures of all records in the zone and the public key are added to the zone in new types of resource records.

The Administrative Burden of DNSSEC

One of the drawbacks of DNSSEC is the additional burden the security extensions place on DNS administrators. Some of the additional administrative tasks include:

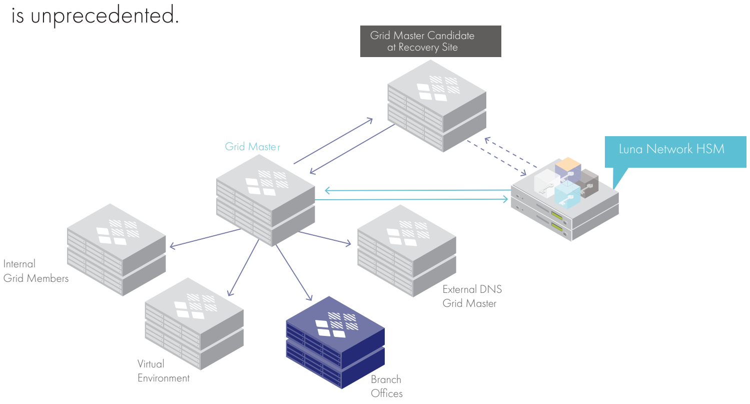
- Key Generation—DNSSEC requires two different keys for each zone—a Zone Signing Key (ZSK) and a Key Signing Key (KSK) 1.
- Signing and Re-signing Zones—DNS administrators need to sign every DNS record in the zone using the ZSK. Any time the zone is changed, the zone needs to be re-signed.
- Key Rollover—Periodically, keys must be "rolled over" to foil cryptanalysis attacks. Note that the administrator cannot just replace the old public keys with new ones. The old one must remain in the zone until all records that were signed with it age out of caches around the Internet.
- Protecting Private Keys—Like any other security model relying on public key cryptography, it is imperative that DNSSEC's private keys are kept secure. By definition, the public key can be made widely available; it does not need to be secured. However, if the private key is compromised, a rogue DNS server can masquerade as the real authoritative server for a signed zone.

Infoblox and the Thales TCT Luna Network HSM Solution for DNSSEC

Infoblox purpose-built physical and virtual appliance platforms combine real-time IP address management (IPAM) with network control, configuration, and change capabilities. The integration between Thales TCT and Infoblox deliver best-in-class IPAM integrated with FIPS 140-2 Level 3-validated HSMs for strong DNSSEC security and simplified key management. The integrated solution has integrated support for DNSSEC and allows single-click configuration, automated key management, and secure key storage. The result is quicker, easier deployment of DNSSEC, lower investment in training and reduced network outages caused by manual key management.

The figure below illustrates such deployment of DNSSEC. Note that the dotted arrow lines are to indicate that the Grid Master Candidate will communicate with the Luna Network HSM for Government only when it has been promoted to Grid Master.

The Infoblox Trinzic DDI DNSSEC solution leverages Infoblox Grid technology, which makes the management and configuration of DNSSEC easier across the DNS infrastructure, often with single mouse clicks. This level of DNSSEC automation, management, and integration is unprecedented.



Robust DNSSEC deployment architecture. Infoblox Grid and Luna Network HSM in high-availability mode.

Automated Management and Configuration

DNSSEC by Infoblox offers central management of all DNSSEC parameters, and allows administrators to enforce standards by configuring DNSSEC parameters at the Grid level. These parameters include default key type, size, and key rollover period; the default values for these are based on the specifications in NIST 800-81 and RFC 4641. Configuring a secondary or recursive name server for DNSSEC can be accomplished with a single click, including enabling DNSSEC on a secondary and enabling validation of DNSSEC on a recursive name server.

Any zone can be signed with a single click by using the "Sign Zone" toolbar button. Keys are generated on the fly and the zone's records are automatically signed—all associated DNSSEC records are automatically created. Signed zones are maintained automatically as well, including ZSK key rollover and zone re-signing. Signed zones are easily identifiable with the DNSSEC icon. DNSKEY, RRSIG, DS, NSEC, NSEC3, and NSEC3PARAM record types are all supported.

Secure Key Management and Key Vaulting

Thales TCT's Luna Network HSMs meet the demanding requirements for robust security and availability required to ensure integrity of the domain namespace. As noted before, one of the biggest challenges in DNSSEC is ensuring the security and integrity of the signing keys (aka private keys). This is where HSMs come into play. HSMs are dedicated systems that physically and logically secure the cryptographic keys and cryptographic processing that are at the heart of digital signatures. HSMs secure the DNSSEC system so the generation of keys, the storing of the private key, and the signing of zones is performed on a server that is physically secure and whose access is restricted to essential personnel only. HSMs also allow the secure storage of backup copies of private keys in a centralized, hardened device.

Thales TCT's Luna Network HSM product line integrates with Infoblox IPAM appliances to provide a certified, tamper-resistant cryptographic platform to perform DNSSEC signing and signature validation, as well as employ secure DNSSEC key generation and lifecycle protection, and key management techniques. These high-assurance services assure the integrity of DNSSEC validation processes and provide robust access controls and event logging. HSMs also support key rollover functions.

The use of DNSSEC increases the number of packets on the network and can decrease the maximum query throughput of the DNS server. Thales TCT's Luna Network HSMs ensures DNSSEC by Infoblox can accelerate to the required additional throughput by offloading the cryptographic operations to the HSM.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

For more information, visit www.thalestct.com