DNSSEC Background Paper
August 2010

Overview

The purpose of this paper is to provide a brief overview of the Domain Name System (DNS), highlight some of the current vulnerabilities to the DNS, and to introduce the Domain Name System Security Extensions (DNSSEC) that will help to mitigate these vulnerabilities.

DNSSEC has been developed to improve the security of the DNS and provide increased protection for activities such as browsing the Internet and email. DNSSEC is in the process of being rolled out internationally. The Internet's root zone was signed earlier this year, and increasing numbers of ccTLDs and gTLDs are now being signed.

This paper does not provide a detailed tutorial of DNSSEC, nor does it provide a guide on how to implement it. The core components of DNSSEC are highlighted in this paper to enable the reader to follow the issues that have been identified in the consultation paper on DNSSEC Implementation.

A reference to DNSSEC specifications can be found at the end of this paper.

Domain Name System

The DNS is a hierarchical naming system for resources, such as computers, that are connected to the Internet or private networks. It is a distributed database that contains mappings of DNS domain names to various types of data such as Internet Protocol (IP) addresses. DNS is essential to the operation of the Internet.

The DNS is often given the analogy of being the *phone directory* for the Internet, as it allows the human readable names to be translated to their IP address.
e.g. dnc.org.nz translates to 202.78.240.52

The domain name space is organised as a tree, with collections of related nodes referred to as zones. Each zone is served by multiple DNS name servers to provide resilience in the event of failure. The .nz name servers are operated by the .nz Registry Services.

Threats to the DNS

Vulnerabilities exist in the DNS and are being actively exploited, allowing miscreants to re-direct, intercept, or modify users' Internet traffic. Each can have potentially devastating consequences, and these attacks are often undetectable to users.

The attacks, which DNSSEC addresses, can be categorised into the following:

- *DNS Spoofing* (malicious cache poisoning)
  This is where a DNS server is manipulated into accepting and caching false data that is not from an authoritative DNS source, and reissues that false data. Examples of cache poisoning include modifying the IP address for a resource, such as a website, or inserting a resource that does not actually exist. The consequence of this is that an attacker can redirect network traffic from the affected domain to a fraudulent destination selected by the attacker.

- *Malicious Resolvers*
  Malicious resolvers pose a threat because the information that they contain cannot be trusted. The consequence is that an attacker can redirect network traffic.

- *Man In The Middle (MITM) Attacks*
  This is where an attacker is able to redirect, intercept, and modify network traffic. Because DNS does not provide any data integrity checks an attacker can intercept and modify legitimate DNS requests or responses destined for the target.

Domain Name System Security Extensions

DNSSEC has been developed to provide authentication and integrity to the DNS to mitigate the attacks listed above, while ensuring that backwards compatibility is maintained.

DNSSEC achieves this through the use of public key cryptography to digitally sign DNS data. DNSSEC-capable resolvers are able to verify whether the data contained in a DNS response comes from an authoritative DNS server and has not been altered.

DNSSEC provides the following improved security benefits to DNS:

- *Origin Authentication and Data Integrity*
  DNSSEC-capable resolvers are able to digitally verify that the DNS data that they received is identical to the information on the authoritative DNSSEC-capable name server.

- *Authenticated denial of existence*
  DNSSEC-capable resolvers are able to determine whether or not a resource, such as a name server, actually exists.

It is worth nothing that DNSSEC does not provide confidentiality of data.

One example of the benefits that DNSSEC provides is that owners of websites and email severs that have implemented DNSSEC will have a higher degree of certainty that visitors to their website and emails destined for their email servers, will not be redirected elsewhere.

Chain of Trust

For DNSSEC to work, resolvers need to be able to fetch the public key and verify that it can be trusted.

The public key to validate a domain name's data, can be obtained from the domains name's authoritative servers. To establish the trust on a key, you can get a copy through an offline trusted channel or use a 'Chain of Trust'.

A 'Link of Trust' is established between a child zone and its parent. The child zone provides a digest of the keys, known as a Delegation Signer (DS) Record, to the parent and the parent validates and signs it, using its own key. The step is repeated up the hierarchy creating a 'Chain of Trust' that can be followed.

For example the Chain of Trust for dnc.org.nz is established through the keys for dnc.org.nz being signed by the .org.nz zone keys. The keys for the .org.nz zone are signed by the .nz zone keys and the keys for the .nz zone are signed by the keys for the root '.' (dot) zone. This forms the Chain of Trust that can be ‘walked’ from the DNS root zone down to dnc.org.nz.

DNSSEC Records

DNSSEC introduces the following new DNS records: DNSKEY, DS, RRSIG, NSEC and NSEC3.

The DNSKEY record contains the public part of a cryptographic key used to sign records in a zone. It usually lives within the zone for a domain name.

The DS record contains a cryptographic digest, a unique digital representation or ‘fingerprint’, of a zone’s DNSKEY and is included in the parent zone. In the case of a domain under .org.nz the DNSKEY is created, and the corresponding DS record is generated and sent to the Registry to be included in the .org.nz zone.

The RRSIG records contain the cryptographic signatures for the DNS data. The NSEC and NSEC3 records are used to provide *Authenticated Denial of Existence.*

How does the secured delegation work?
The DS record holds the digest of a child's zone key and is signed with the zone key from the parent. By verifying the signature of the DS record, a resolver can validate the digest of the child's zone key. If the digest is successfully validated then the resolver can compare it with the digest of the child's zone key. If the two digests match then the child's zone key can be used to validate the DNS data in the child zone.

Management of DNS and DNSSEC Keys

As DNSSEC uses public key cryptography the existence and management of cryptographic keys for each domain name that implements DNSSEC is required.

Registrants can elect to operate their own DNS or they can delegate this responsibility to a third party called a ‘DNS Operator’. The DNS Operator could be the Registrar for the domain, a Registrar who does not manage the domain, a hosting provider, an ISP, or some other third party that offers DNS management services.

Once DNSSEC has been implemented on a domain name and it's DNS records have been signed, at some point in the future changes to the DNS data may be needed. The changes may be DNSSEC related such as updating the key used to sign the data, or transferring a domain name registration to another Registrar.

When these changes are made they will need to be properly managed and additional steps are required to ensure that resolution errors do not occur. Resolution errors may result in DNSSEC-capable resolvers being unable to verify the information that has been sent to them, and this may result a domain being unreachable for a period of time.

Example Scenario

The following scenario has been prepared to illustrate how vulnerabilities in the DNS are being exploited by miscreants and how DNSSEC mitigates those threats.

The goal of the attacker is to redirect the customers of a banking website to a fraudulent website, under the attacker's control, to harvest customer's credentials. In the following scenario neither the target bank or ISP have implemented DNSSEC.

- The attacker sets up a fake banking website that looks identical to a legitimate bank's website.
- The attacker then poisons the cache of an ISP's DNS servers, with the IP address for their fake website.
- When any customers of the targeted ISP enter the website address for the targeted bank into their browser, the ISP's DNS server provides the customer with the fraudulent IP address, redirecting their customers to the attacker's website.
- When the customers log into the fraudulent website their usernames and passwords are captured and recorded by the attacker.
- The attacker then uses those credentials to log into the targeted banks website, masquerading as a legitimate user, and transfer the funds to an account they control.

In this scenario if either the bank or the ISP had implemented DNSSEC then the ISP's customers may not have ended up being redirected to the attackers fraudulent website.

- If the bank had implemented DNSSEC, the customer's computer may have detected the fraudulent IP address when it attempted to validate the response from the ISP's DNS server.

- If the ISP had implemented DNSSEC then the ISP's caching server would have rejected the attempt to poison its cache.

Two real world examples similar to the example above can be found here:

- Brazilian Bank Bandesco
- Irish ISP Eircom

DNSSEC Related Specifications

The following is a list of RFCs that define the current version of DNSSEC, and are provided for further reading:

- RFC 4033 - DNS Security Introduction and Requirements
- RFC 4034 - Resource Records for the DNS Security Extensions
- RFC 4035 - Protocol Modifications for the DNS Security Extensions
- RFC 4641 - DNSSEC Operational Practices
- RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

As the .nz DNSSEC project progresses resources for Registrants and Registrars, such as an FAQ section, will be added to the DNCL website.