Steps Towards Implementing DNSSEC

The Domain Name System is an essential part of the Internet. Here, we look back on the role of DNS, and examine the challenges and future prospects for the implementation of the DNSSEC technology that responds to the threats to DNS that are of concern today.

2.1 The Role of DNS

DNS is a service that simply returns resource records in response to queries, but this service is indispensible for the operation of the Internet. For example, though users themselves are seldom aware of this, everyday Internet usage such as the viewing of pages on a Web browser or the sending and receiving of email rely on DNS behind the scenes. Of course, DNS is not required for communications. However, due to factors such as the need to remember the IP address of the other party, the usefulness of the Internet is greatly hampered without DNS, and it is realistic to say that many users are dependent on it.

DNS enables the distributed management of the Internet, dividing it into areas known as zones. The top level of the Internet is the root zone, which is represented by a period (“.”). By setting subdomains as needed and delegating their administration, a tree-like hierarchy of distributed management is formed. For example, the .jp country code top-level domain is administered by Japan Registry Services Co., Ltd., and all registered .jp domains are published through a group of content DNS servers called JPDNS. When queries are made, the required resource records are located via this tree-like hierarchy of content DNS servers that are delegated to other organizations and managed in a distributed manner.

In many cases the user’s terminal does not handle this process itself, but rather sends a query to a cache DNS server operated by an ISP or network administrator. The cache DNS server responds to the terminal’s query by locating the content DNS server, searching for the required resource records, and returning the results to the terminal. If DNS is not operating correctly, it results in the target service being rendered inaccessible. Incidents of websites not being accessible due to problems with DNS actually occur quite often worldwide.

2.2 The Need for DNSSEC

The most insidious problem with the operation of DNS servers is false responses. When an incorrect resource record is sent back in response, the party receiving this response is likely to trust this information, and due to the mistaken details a great deal of trouble can be caused. As some people have harmful intentions, attacks that inject these false responses intentionally have been known to occur. When these attacks succeed, it is possible to lead users attempting to access certain websites to completely unrelated sites of the attacker’s choosing. It is easy to imagine

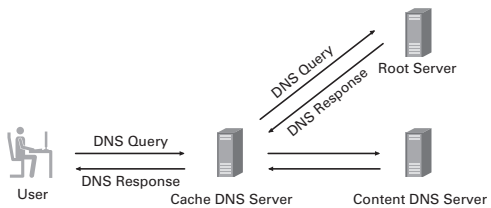

Figure 1: DNS Queries and Responses

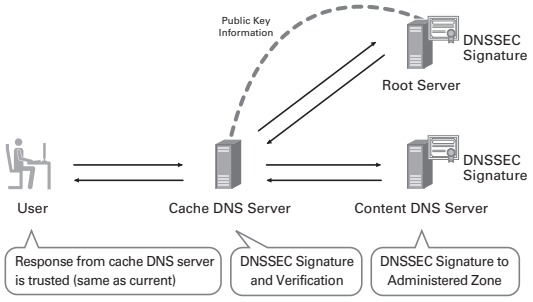

Figure 2: DNSSEC Implementation

how this could result in problems such as the stealing of account information. To make matters worse, these attacks are possible using the terminals and Internet speeds available today.

With these kinds of attacks in mind, related parties have been evaluating the implementation of a technology called DNSSEC, which makes it possible to verify whether or not a DNS response is legitimate. DNSSEC authenticates the sender of a response by attaching a digital signature that uses a public key encryption method to DNS responses, making it possible to confirm the integrity of a response.

Under DNSSEC, digital signatures are created for each zone. Public key information is required to verify these signatures. With DNSSEC, it is possible to register the public key information used in signatures on a subdomain to a zone as a resource record. By doing this, when the public key information for a certain zone is acquired, it is possible to carry out verification for its subdomains by following the registered public key information. This chain of trust makes it possible to verify DNSSEC from any given zone, and as long as the chain of trust is not broken and the root (.) public key information is acquired, all signed zones can be verified.

2.3 Work Towards Support for DNSSEC

When considering support for DNSSEC as the administrator of a zone, two tasks are required. The first is the signing of the zone, and the second is the registration of the public key information used with the signature to the higher level zone. The signing of a zone is closely related to key operation, and requires knowledge of public key encryption and ongoing updates and signing of keys. Additionally, when public key information is registered to the higher level zone, the registry administering that zone and the registrar serving as the point of registration must also of course support DNSSEC. The .jp country code top-level domain began DNSSEC signatures for the JP zone on October 17, 2010. Registry support, meaning the start of acceptance of public key information registration, is scheduled for January 16, 2011.

On the query-handling side, it is thought that the model to be adopted will involve DNSSEC verification first being carried on a cache DNS server operated by an ISP or network administrator, with terminals trusting these verification results. The cache DNS servers that carry out this DNSSEC verification must acquire the public key information to serve as the basis of trust for the domain to be verified. With the root (.) zone now DNSSEC signed, setting the root zone's public key information would be a straightforward method of operation, but depending on operating policies it should also be possible to limit verification to the required area only. In either case, this public key information must be updated in conformance with the timing of updates to the key itself.

There have actually already been many reports of problems relating to the operation of DNSSEC. These range from simple cases in which updates were neglected to those in which there were issues with the operation tools. When problems with DNSSEC occur, in most cases the signature verification process will fail, and the cache DNS server will return an error. This means that the user will not receive the required response from the DNS. In actual fact, the problems mentioned above had a significant impact on operations, with many users not able to access websites. Though the goal of implementing DNSSEC is to improve security, if it cannot be operated properly, it causes issues such as rendering sites inaccessible.

DNSSEC requires knowledge of public key encryption and ongoing update work, and demands stricter operation of DNS than before. Unfortunately, this means that at present it is not something that can be implemented easily. Despite this fact, a function that enables verification of DNS responses is of great importance, and for services that may face considerable damages when a DNS response is forged, it is worth considering creating an operating framework and implementing this technology. IIJ has carried out a various trials and surveys working towards the implementation of DNSSEC. We have also actively cooperated in the implementation of DNSSEC on a number of top-level domains. We hope to put the knowledge we have gained to use in providing a safer Internet environment through DNSSEC.

Author:
Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Technology Promotion Section of the Network Service Division in the IIJ Network Service Department. Mr. Matsuzaki is always finding things that pique his interest while striving at his work. He is an IIJ-SECT member, co-chair of The Asia Pacific OperatorS Forum, chair of APNIC IPv6 SIG, and an expert advisor for JPCERT/CC.