Domain Name System

Date: 22 Oct 2017

Organisation: Hong Kong Computer Emergency Response Team Coordination Centre

Domain Name System (DNS) is widely used on the Internet. It provides domain name and IP address mapping, making human access to Internet become easy without the need to remember IP address. DNS was invented in 1983. At that time, security design was not a major concern. As a result, DNS is vulnerable to hacker attack nowadays.

DNS attacks include "man-in-the-middle", "DNS cache poison", "DNS proofing" and "fake DNS servers" etc. DNS attack can be successful because the protocol itself is lack of authentication in both DNS queries and responses. Hackers can create fake DNS packets to reply wrong IP address, then redirect users to fake website site.

There have been some incidents about domain attack, such as “google.com.my” and “google.my” domain name by DNS cache poisoning, redirecting users to fake google site. In 2015, Malaysian Airlines (MAS) domain name server was compromised and domain name records were changed, similarly redirecting users to fake web site.

As early as 2000, it has been suggested to use Domain Name System Security Extension (DNSSEC) to enhance the data integrity of DNS service. Until 2007 the top of the domain root "." officially started to support DNSSEC, after that other top-level domains (TLD) followed, eventually in September 2017 ".hk" top-level domain also officially supported DNSSEC.

DNSSEC uses digital signature of public-private key encryption technology to verify the domain name record. It uses private key to sign the DNS record and uses the public key to verify the response come from official source and the content of the record to determine whether information is tampered or not. In order to prevent the public key be spoofed, the signature of the public key is placed in the Parent Zone. So there are many layers of verification, constituting the entire DNS chain of trust and therefore hackers are difficult to attack.

The Hong Kong Computer Security Incident Coordinating Center recommends all domain name administrators to build DNSSEC to enhance the integrity and credibility of their domain records, and contribute to fight on cybercrime.