Security for Future Internet Architecture - Motivation from DNSSEC

Pokai Chen
Department of Computer Science
National Chiao Tung University
Email: pokai@dsns.cs.nctu.edu.tw

Shiuhpyng Shieh
Taiwan Information Security Center at NCTU (TWISC@NCTU)
Email: ssp@cs.nctu.edu.tw

Abstract

DNS has a long history of being the primary target of malicious network attacks. These attacks take advantage of the weakness that the domain name mapping information is not authenticated. This motivates the need of security global infrastructure for future internet architecture. DNSSEC is a secure extension of DNS, and is considered as one of the most important mechanisms for critical information infrastructures protection (CIIP). In this article, we will investigate the substantial impact of DNSSEC deployment in the Internet architecture, and new opportunities may arise in response to the debut of this new security network infrastructure.

Domain Name Server

Domain Name System (DNS) [1][2] is one of the most important infrastructures for the Internet. DNS provides the service that facilitates the mapping between IP addresses and domain names, such as host names, email addresses, and Uniform Resource Locators (URLs). With DNS, users do not need to memorize the clumsy IP address of their target server but instead use the hostname that is easy to remember. DNS also provides some advance functions like robust host mapping and load balancing. In fact, DNS is used not only for mapping information between IP address and hostname, but also for other naming services. An important feature of DNS is its distributed and far-reaching structure. DNS is designed with hierarchical architecture and the management authority of DNS sub-domain is delegated top-down to many different organizations. For example, the organization which manage root domain name servers delegates another organization to manage ".org" domain; and the ".org" organization delegates another organization to manage "example.org" domain; "example.org" organization has the authority to set "host1.example.org", "host2.example.org", etc. With this hierarchal architecture, the authority of managing DNS domains is divided into many different organizations. Each authoritative server is responsible for handling the domain names under its jurisdiction. Users can get connected from its local domain name server, namely resolver name server, to these sub-domains through authoritative relationships. This robust architecture makes DNS as one of the most crucial information storage and retrieval infrastructures

Secure DNS - DNSSEC

As many ancient protocols, DNS is not safe. Hackers may use various techniques to masquerade as a DNS server to issue DNS packets to mislead and attack users [3]. Recently, DNSSEC [4][5][6] is developed to resolve DNS security problems. DNSSEC is an extension standard of DNS. It associates the digital signature based authentication scheme with DNS. With the authentication mechanism, hackers cannot forge DNSSEC packets, but users can authenticate and trust DNSSEC packets. DNSSEC improves security of DNS by providing origin authentication and data integrity. Consequently, a hacker cannot disguise himself as an official DNSSEC server, and also cannot modify the DNSSEC packets through man-in-the-middle attacks between users and DNSSEC server. DNSSEC prevents the phishing attack by protecting the mapping information of domain names and IP addresses.

Certification

DNSSEC protects various types of data. Among them, a type of DNSSEC data is particular of great importance and will have significant impact to future internet security, that is, certificates. According to RFC 4398 [7], the administrator of example.org domain can create a certificate for machine “host1.example.org”. This certificate can be stored on the authoritative DNSSEC server of “example.org” domain. When a user intends to retrieve this certificate, he knows where to request for it. Not only certificates designated for hosts and network access interfaces can be stored in DNSSEC servers, personal certificates can be preserved in the same way. According to RFC 2822 [8], the email address of “user@example.org” can be translated to “user.example.org”. Therefore, when any user wants to query for the certificate of “user@example.org”, he can request or “user.example.org” as a normal DNSSEC query. This personal certificate can be used for secure email protocols such as S/MIME [9] and OpenPGP [10]. In the similar fashion, it also can be used as an individual identity in any network application.

Authentication and Trusted Path

DNSSEC global information infrastructure provides a trusted tunnel among the DNSSEC servers for the storage, propagation, and inquiry of certificates. The DNSSEC infrastructure can be considered as a vehicle for public key infrastructure (PKI) and the distribution of certificates among the DNSSEC servers can be trusted. Certificate authorities (CAs) do not need participate in the certification distribution and key verification among DNSSEC servers. The DNSSEC infrastructure guarantees that the certificates and the domain names stored in a local resolver DNSSEC server have been authenticated and verified when they were retrieved from remote authoritative DNSSEC servers.

The secure mechanism of PKI is based on trusted third party attestation and transitive

relationship. If users trust a CA certificate, then they can trust transitively all the certificates issued in the trustworthy hierarchical tree. DNSSEC uses the similar trustworthy hierarchical architecture but the trustworthiness relies on server attestation instead of certificate attestation. The business models of server attestation and certificate attestation are very different. For certificate attestation in the hierarchy, upper-level CAs charge lower-level CAs for attesting them. However, the domain name service is provided for free on the Internet, and the Internet is still lack of a global PKI. The advantage of building global server-attestation based certification infrastructure on DNSSEC is that DNS has been in place and mature for a long time. The DNS relationship between upper and lower level organizations is already well defined. All computer systems and networks heavily rely on the DNS infrastructure. If organizations can publish certificates of their domains through the trustworthy DNSSEC infrastructure for free, the increasing popularity of certificates can be expected. Hence, many new secure internet applications based on certificates can be widely deployed.

Vehicle for Secure Network Applications

Taking email as an example, although secure email systems, such as S/MIME and OpenPGP are solid and mature technology for a long time, they are still not so widely used as conventional insecure email systems. The main reason is the lack of global authentication infrastructure. These secure network applications are based on certificates, however, global PKI is still not in place. With DNSSEC, organizations can provide certificates to their members at low cost. If every user has a certificate for his email account, the recipient can authenticate the sender of an email by verifying its digital signature. Consequently, spam mails can be filtered and forged emails can be detected and removed.

DNSSEC will soon become the vehicle of global public key infrastructure. This will motives the deployment of many new network applications, such as online shopping, online banking, forum, and social web site, that requires authentication, integrity, non-repudiation, confidentiality, and privacy. On the other hand, these certificates can be used to facilitate the establishment of secure IPSec tunnels among network devices. The global deployment of public key infrastructure may overturn the innate insecurity of TCP/IP networks.

Some operating systems such as Window 7 has been designed to partially support DNSSEC. On the other hand, DNSSEC servers have been deployed at fast pace. The global DNSSEC root and some country domains are already in operation, including root domain, .net domain, and .org domain. .com domain will start its operation of DNSSEC in March 2011. With DNSSEC infrastructure in place, a more secure future Internet architecture can be expected for the years to come.

Conclusions

Critical Information Infrastructure Protection (CIIP) is crucial for the protection of network users and applications on the Internet. In CIIP, DNS has been the primary target of adversaries. To cope with the problem, DNSSEC has been proposed to provide a trusted path for the distribution of domain name information and digital certificates. DNSSEC can be a vehicle for the trusted distribution of digital certificates. With the global security infrastructure in place, the deployment of many new secure applications become possible.

Acknowledgement

This work is supported in part by National Science Council, NCP, TWISC, ITRI, III, iCAST, Chungshan Institute of Science and Technology, Bureau of Investigation, and Chunghwa Telecomm.

References

[1] P. Mockapetris, "Domain Names – Concepts and facilities," *IETF RFC 1034*, Nov. 1987.

[2] P. Mockapetris, "Domain Names – Implementation and Specification," *IETF RFC 1034*, Nov. 1987.

[3] D. Atkins and R. Austein, "Threat Analysis of the Domain Name System (DNS)," *IETF RFC 3833*, Aug. 2004.

[4] R. Arends et al., "DNS Security Introduction and Requirements," *IETF RFC 4033*, Mar 2005.

[5] R. Arends et al., "Resource Records for the DNS Security Extensions," *IETF RFC 4034*, Mar. 2005.

[6] R. Arends et al., "Protocol Modifications for the DNS Security Extensions," *IETF RFC 4035*, Mar. 2005.

[7] S. Josefsson, "Storing Certificates in the Domain Name System (DNS)," *IETF RFC 4398*, Mar. 2006.

[8] P. Resnick, "Internet Message Format," *IETF RFC 2822*, Apr. 2001.

[9] B. Ramsdell and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," *IETF RFC 5751*, Jan. 2010.

[10] J. Callas et al., "OpenPGP Message Format", *IETF RFC 4880*, Nov. 2007.