2023 Spring CNS Reading Critique #6

DNSSEC VS DoH(DNS-over-HTTPS)

R11921A16 何秉學

I. Summary of DNSSEC

DNSSEC is a security extension protocol designed to protect the security of information during domain name resolution. It uses public key encryption technology to sign and verify data in the network DNS, thereby ensuring the integrity and authenticity of the data. DNSSEC provides a mechanism for clients to verify whether the DNS resource record (such as IP addresses, email addresses, etc.) they requested is from the correct source and has not been tampered with. This effectively prevents security issues such as DNS cache poisoning attacks and DNS hijacking. DNSSEC plays an important role in protecting Internet security, and many government agencies, financial institutions, and businesses have begun to deploy DNSSEC.

II. Summary of DoH

DoH is a mechanism that encrypts DNS queries over the HTTPS protocol. Its purpose is to improve the reliability and efficiency of DNS queries while increasing privacy and security. Traditional DNS queries are in plaintext and vulnerable to eavesdropping and interception. Using DoH, DNS queries are encrypted, protecting users' privacy and data security. DoH can also prevent DNS cache poisoning attacks and DNS hijacking, improving the security of DNS resolution. DoH can also help network providers reduce a load of DNS queries, improving network performance and speed. Since DoH is transmitted via the standard HTTPS protocol, it can more easily pass through corporate and organizational firewalls and is not blocked or restricted by ISPs.

III. Comparison

Both of them can prevent DNS cache poisoning attacks and DNS hijacking attacks and enhance the security and reliability of DNS queries. Also, they can preserve the privacy of users, e.g., DNSSEC can avoid DNS man-in-the-middle attacks and data tampering and DoH can encrypt DNS queries, protecting users' privacy and data security, preventing DNS eavesdropping and interception. However, they still have some drawbacks to conquer such as the implementation of DNSSEC and DoH are complex and requires special configuration and management. Moreover, if DoH or DNSSEC is used, it may increase network congestion and delay, because it needs to use HTTPS protocol (for DoH) to encrypt and decrypt DNS queries.

IV. Reflection

If I were the author, I would consider conducting more experiments and evaluations to validate the effectiveness and performance of these technologies in different scenarios. I would also explore ways to enhance their interoperability with other security technologies and ensure their widespread adoption and implementation. There are still some unsolved questions regarding DNSSEC and DoH, such as the challenges of key management, the potential impact on network performance, and the trade-offs between security and usability. Further research is needed to address these questions and refine these technologies.