**Understanding DNSSEC**

Domain Name System or DNS acts as the phonebook of the world of the internet by converting user-made domain names to machine-understandable IP addresses. The functionality of the internet is correlated with DNS. But the use of DNS is not very secure. DNS never checks whether an address is authenticated or not. Thus, there are chances of fraudulent attacks on DNS.

To battle this problem, the concept of DNSSEC was introduced. DNSSEC or Domain Name System Security Extensions solves this issue by adding an authentication surface to this.DNSSEC was introduced back in the 90s by a group of people working in the organization responsible for the DNS protocols. The authentication process is made secure with help of public key cryptography with the use of a digital signature.

Every DNS zone has a pair of private and public keys. The holder uses the private key to sign the data and generate the digital signature of that data. This private key is only known to the owner and none else. But on the other hand, public keys are used by everybody and are accessible publicly. DNS data is authenticated with the use of a private key. It confirms whether the digital signature that is generated with the help of a private key is valid or invalid.

Two very essential features are added to the DNS protocol by DNSSEC.

1)The use of authentication helps to identify whether the data is valid and is coming from the source it is claiming to be coming from.

2)The integrity features help to understand whether there has been any modification to the data in the middle of the transfer.

**Why is DNSSEC needed?**

The concept of DNSSEC was introduced to overcome the disadvantages that are possessed by DNS. The need for DNSSEC in today’s internet-driven world is huge. Some of them are as follows.

1)The authentication process helps to identify valid data and make sure that the source from where the data is coming is authorized and the same as claimed.

2)It prevents the user from getting invalid data by identifying the valid ones and blocking the invalid ones.

3)With the use of public and private keys, data confidentiality is maintained.

**How does this work?**

Using a digital signature based on private and public key cryptography, this works. The process is a simple one and is as follows.

1)The holder of the organization generates a private key that is accessible to them.

2)The domain registrar is then sent the generated public key.

3) The key is then sent to the registry which checks the key.

4)At last the registry signs the key and publishes it for all the users to access.

**Reasons for not using DNSSEC by the majority of business firms**

Although the use of DNSSEC has a lot of positive impact on the overall security of the internet ecosystem, still this is not used by many business firms today. Among the various CAC40 business firms, roughly 4-5 companies use this protocol. There are various reasons for this less usage. Although the reasons are pretty simple to comprehend.

1)DNSSEC is a manual implementation process and this execution is not a very simple task. It is somewhat a complex process that makes the firms keep a distance from it.

2)Regular maintenance of this protocol is another disadvantage which has a lot of complexity while handling.

3)Small errors in terms of technicality can give rise to huge discrepancies.

**Why is it important?**

1)The most important task of DNSSEC is to prevent unauthorized DNS data from entering and causing any kind of harm and discrepancy to firms.

2)It provides an extra layer of security to the already existing DNS system.

3)The integrity feature makes sure that there are no changes or modifications that are done to the data.

**References**

1.<https://www.arvancloud.com/blog/en/what-is-dnssec-why-is-dnssec-important/>

2.<https://www.internetsociety.org/deploy360/dnssec/basics/?gclid=Cj0KCQjw9ZGYBhCEARIsAEUXITX0U7EBvJ0_K2JPIGVnJVLyuOvK3XWhq6PJ6d72_FTZoHSu1kdQ1OMaAg_oEALw_wcB>

3.<https://www.csoonline.com/article/3569277/dnssec-explained-why-you-might-want-to-implement-it-on-your-domain.html>

4.<https://mediatemple.net/blog/web-development-tech/what-is-dnssec/>

5.<https://umbrella.cisco.com/blog/what-is-dnssec-and-why-is-it-important>

6.<https://ctovision.com/what-is-dnssec-and-why-is-it-important/>

7.<https://www.cloudflare.com/en-in/dns/dnssec/how-dnssec-works/>