Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Security and Privacy

ER -5

Declaration: "I have read, and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at http://www.tcd.ie/calendar. I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write,' located at http://tcdie.libguides.com/plagiarism/ready-steady-write."

Submitted By

Harsh Dhingra

19323904

Q5 (a)

DNSSEC is Domain Name System Security Extensions are protocols for securing the particular type of information provided by the DNS (Domain Name System).DNS converts or translates the human-friendly domain name (such as amazon.com) to IP addresses(192.123.12.3) which are needed by server and other network routes across the internet. DNS isn't secure enough and possesses various threats, e.g., cache-poisoning attack. This resulted in the development of DNSSEC (by the engineers in IETF)

DNNSEC strengthens the DNS using digital signatures which are based on public-key cryptography. DNNSEC also provided data integrity; therefore, the bottom line is that the DNSSEC protects against spoofing of DNS data. DNSSEC helps in preventing DNS cache poisoning; it detects DNS data corruption or manipulation on authoritative DNS servers; in this, Man-in-the-middle (MITM) attacks are also detected.

Whenever DNSSEC is used, each DNS request contains an RRSIG (Resource Record Signature, a digital signature of the requested DNS data) and the requested record type. This digital signature key is verified by locating the correct public key from DNSKEY (Contains the public key that a DNS resolver uses to verify DNSSEC signatures in RRSIG records.). NSEC and NSEC3 are providing cryptographic evidence of the nonexistence of any request. This process is also known as authenticated denial of service. DS (delegation signer) is being used for the authentication of DNSKEY's, and this is called chain of trust. In DNSSEC, each zone has a public/private key pair, and the zone's public key is stored in the new DNSKEY record; the zone's private key is kept safe offline. DNS data is signed by each zone's individual private key in that zone, which creates a digital signature that is also published in DNS. It uses a very rigid trust model and there is a chain of trust that flows from parent zone to child zone. The first public key of a chain of trust is called the trust anchor.

Therefore the DNSSEC provides Data Origin Authentication – which allows a resolver to verify data received from the requested zone, and Data Integrity Protection – which allows the resolver to know that the data was originally signed by the zone owner's private key and it hasn't been modified in transit. If any of the above features is exploited the resolver assumes it as a cyberattack and discards the data and returns an error.

Since DNSSEC only aims to protect Data Integrity and Authenticity, therefore we can see various flaws in DNSSEC –

(1) Its cryptographically weak – since its first draft are from 1994; therefore, it relies on RSA with PKCS1v15 padding, and the deployed system is littered with 1024-bit keys
(2) It is expensive to adopt – since there isn't wide use of DNSSEC, it lacks connectivity over the internet, not universally supported on all-recursive servers
(3) It is expensive to deploy
(4) Each time you change the zone, you must resign it, and the keys must be rotated regularly.
(5) Zone Walking – which is a threat to network security
(6) To build a chain of trust, the zone owner needs to manually over the chain from parent to child zone

Q5 (b)

DNSSEC has excellent advantages, and it also addresses the security limitation of the original DNS protocol. Still, unfortunately, we can see that the deployment of DNSSEC is very low, i.e. about 3% of names signed, less than 2% of .com second-level domains. Though DNSSEC is already criticized in Q5(a) but the following reason clears us about the low deployment: There are a high fraction of domains with DNSKEY's missing DS records – installing DS records is a tiresome process because DS records are uploaded to the parent zone via registry, and the domain owner can't directly access it, only a registrar has access to it. So, the bottom line is that for any domain that supports DNSSEC, its registrar must provide an NS recordset as well as a DS record to the registry. (NS recordset is the identity of authoritative nameservers of the domain name).

The following plan should be adopted to increase the deployment of DNNSEC:

1) All the present DNS entities such as registries, registrars, and third-party operators should be encouraged to deploy DNSSEC, they should be given some financial incentives such as free DNSSEC for customers, This would increase the usage of DNNSEC significantly.
2) The registrars should provide DNSSEC domains either free or at a discounted price. Considering OVH and GoDaddy- OVH provided DNSSEC for free and the latter has a premium price for it- it is seen that OVH's overall DNSSEC adoption rate is over 25 percent and is increasing – which means customers are really into it.
3) DNSSEC should extend its services to third-party DNS operators. Currently, third-party operators generate DNSKEY's and DS records, but customers have to provide the record to the registrar; the third-party operator has no authority over it.

Q5 (c)

If I am dishonest, I would like to have access to these keys given below:

Zone Signing Key(ZSK) – It's an authentication key that is used to sign a zone.

Key Signing Key(KSK) – Its an authentication key used to sign one or more signing keys of a zone. The private key of KSK signs ZSK.

CSK (Combined Signing Key) –combines the functionality of ZSK and KSK. And acting as a single key, it has both roles of ZSK and KSK i.e, signing the zone as well as linking parent and child zone

Each zone in DNSSEC has ZSK, and its private part is used to verify/digitally sign each RRset. Now the Key signing key signs the ZSK, and this is how a chain of trust is built. Now since it is all verified, we can make a malicious site for the zone

References

[1] https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/

[2] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn593682(v=ws.11)

[3]https://bind9.readthedocs.io/en/latest/dnssec-guide.html#advanced-discussions-key-generation

[4] https://cdns.net/DNSSEC.pdf