At-Large Summit Workgroup 5

DNS Security Issues within ICANN's Remit
Collection of questions about DNSSEC

Text prepared by Lutz Donnerhacke, Chair of the Summit Working Group 5

Is DNS at risk?

The previous DNS protocol is subject to a number of threats. It is particularly vulnerable to spoofing attacks. Such an attack could be used to redirect unsuspecting users to a malicious site, or redirect email through the attackers system. Increasingly sophisticated attacks run against the DNS, and it's likely that they will increase in number and severity in much the way as viruses and worms have.

What is DNSSEC?

DNSSEC is a set of extensions to the DNS that permits authentication and data integrity checking of DNS data.

How does DNSSEC work?

DNSSEC doesn't modify the existing ressource records stored and retrieved; it simply adds additional records to the DNS data which permit the validation of data in the DNS using strong public key cryptography. Any validating resolver does announce it's capability in each DNS question to receive the additional records. So the system is backward compatible. On the other hand an intermediate validating resolver can be queried to bypass the verification; so the end-to-end principle remains intact while protecting security agnostic system like computers in the LAN or broadband customers of an ISP can be centralized. In the case of attacks, the validating resolver simply returns an unspecified error instead of the faked answer.

Will DNSSEC change the usability of DNS?

DNSSEC allows to trust the data stored in the system, so it turns a distributed hierarchical database into a trustworthy decentralized data store safe to put security-related data in the DNS, e.g. X.509 certificates, SSH fingerprints, and OpenPGP keys. This new DNS provides a extensible public key infrastructure (PKI) for free.

Which new security and privacy risks are opened by DNSSEC?

The additional records increase the size of DNS answers, which causes problems to older software as well as make it suitable tool for DDoS attacks. Some versions of DNSSEC allows to traverse the zone content; beside the data is public anyway, some privacy issues arise. In those cases an modified signature (NSEC3) should be used.

Does DNSSEC require trusted servers and operators?

Only the signing a zone required a trusted environment. All other hosting and transporting devices may run in the usual way without weakening the security. Any modification will be detected, malicious systems will be sorted out.

Who can sign a zone and who needs to be asked or informed?

Every zone administrator may sign it's zones without asking. If the parent zone is already signed, the zone administrator should inform the parent operators about the currently used keys in order to ease external verification. Regardless of the parent zone, the administrator may distribute the zone keys himself, or put them into available third party trust anchor repositories also know as DLV registries. Because distributed keys are hard to change, the recommended scheme is to use zone signing keys (ZSK) for daily work and distribute more sensibly handled key signing keys (KSK) which only signs the ZSK in the zone.

Is it necessary to sign the root?

Technically the existing trust anchor repositories can be used instead of a signed root, but a signed root is much more likely to be validated, it's much easier to insist in validation as a customer, and DNS mangling activities (like DNS censorship) will fail while testing the concept.

Is it necessary to sign the top level domains?

TLDs are huge domain concentrators, if they are not signed, a lot of keys needs to be distributed manually or via trust anchor repositories. Such large scale out of band communication must fail for a considerably amount of zones. That's

why all TLDs should be signed.