

DNSSEC for .at

nic.at position

1 Introduction

The Domain Name System (DNS) is one of the most important protocols on the internet. DNS maps names like `www.nic.at` to the corresponding IP-addresses. This allows to find the webservice of a domain, enables the delivery of e-mails and also voice-over-ip calls – almost any service on the internet as of today makes use of DNS. From the viewpoint of an internet user, DNS outages are equivalent to a “whole internet failure”; they can not reach websites, they can not send e-mails and their instant messaging application don't work anymore. DNS is an important basis for almost all internet applications like surfing, mailing, etc.

If an attacker manages to inject false information into the DNS, he'd be in a position to redirect users to rogue websites or spy on e-mails of other users. DNS implements some security features to prevent such scenarios, but the security features have become weaker with increased availability of bandwidth, and can easily be bypassed. The basic design of DNS is over 20 years old, although in the last year some extensions have been standardized to raise the security level.

One of the most discussed new techniques is DNS Security Extensions (DNSSEC). DNSSEC increases the security in the DNS-system, but at the same time the complexity and the possibilities for errors also increases significantly. DNSSEC demands a rethinking or even a complete redesign of existing business processes in the registry/registrar/registrant-business.

Nic.at, experienced registry operator for the .at ccTLD and a competent partner for all DNS questions, participates in the development of DNS and runs a lab to test new DNS-technology like DNSSEC. Nic.at performed a lot of testing on DNSSEC, and this paper gives a short overview about the problems of DNSSEC and the position of nic.at for the deployment of DNSSEC within the .at ccTLD.

2 DNSSEC Problems

DNSSEC addresses a major design flaw in the DNS: clients could not verify the answer of a nameserver. DNS does not allow for verification, whether or not the DNS response has been modified during transport. DNSSEC addresses this problem by adding a digital signature to the DNS response, which can then be verified by the client with a Public-Private-Key method. This ensures that the DNS-answer contains the correct data. However, the data is only signed, not encrypted.

In theory DNSSEC is a good solution to solve weaknesses in the DNS-protocol and increase the security and trust in DNS. Unfortunately in reality some problems occur; particularly because the DNSSEC deployment has to be done in a live environment – the global DNS. These problems make the use of DNSSEC in such a critical system like DNS problematic. As mentioned above DNS is a very critical service in the internet and even a short outage is not tolerable.

Nic.at has identified the following major problems:

Root zone not signed

The DNSSEC concept is based on a fully signed DNS-tree. The most important element is the signed root zone, which is the entry point for the chain-of-trust. The chain-of-trust enables the client to verify the received keys for a zone by “walking down” from the top. There are plans to sign the root zone at the end of 2009/ at the beginning of 2010, but currently the root zone is not signed.

There are workaround solutions available for this problem (like IANA Interim Trust Anchor Repository (ITAR) or ISCs DNSSEC Look-aside Validation (DLV)) but those solutions require additional administration work and software support.

Status of DNSSEC Software

DNSSEC is a rather new technology and the support for DNSSEC in DNS software varies. Two of the most popular DNS-Server (Bind and NSD) support DNSSEC since some time, but each new release of the software contains a lot of bugfixes for DNSSEC – an indication that support is not extremely stable at this point in time. Each protocol standard (and especially such a complex standard like DNSSEC) allows for diversity when implemented. It takes some time until the interoperability between software from different vendors is established. Some parts of DNSSEC have been standardized later (like NSEC3) and are only supported in the newest versions of the software.

Microsoft will only support a part of DNSSEC (only NSEC, no NSEC3) in Windows 7 and Windows Server 2008-R2; for older version there is no DNSSEC support planned.

DNSSEC requires ongoing administration

Without DNSSEC it is possible to configure the authoritative Nameservers once, register the domains with the registry and let the system run on “autopilot” without any additional administration required. With DNSSEC this is impossible. DNSSEC-signatures are only valid for a period of time and have to be renewed. The keys used to generate the signatures should be rolled over periodically to avoid compromise of the keys via brute-force attacks. DNSSEC therefore isn't a plain software update.

Fault tolerance of DNS decreases

DNS is a very fault tolerant protocol. As long as at least one nameserver for a zone is reachable DNS will work. There is a big grey area, where DNS will work although there are a lot of errors (wrong configuration, unreachable nameservers ...). With DNSSEC this grey area gets very small - If there is something wrong with the keys or signatures the zone cannot be resolved any more.

Especially the key rollover has a big potential for fatal failures. If a failure happens and wrong keys are floating around it will take some time until the problem is solved; resolving nameserver may cache the wrong keys and attempts to validate the signatures which will fail.

Once a zone is signed with DNSSEC it not easily possible to switch back to a non-DNSSEC zone. A lots of timing-critical steps have to be performed, just removing the keys and signatures from a zone is not enough.

Support problems

Customers typically use the resolving nameservers provided by their ISP. If an ISP enabled DNSSEC-validation on his nameservers and a big company encounters problems with their DNSSEC-setup (like for example google sign their zones with a wrong key) the zone could not be resolved by customers and all those customers would likely contact their ISP. So the ISP has the problems with his customers for a problem he can't resolve (except by reverting their DNS to DNSSEC-validation off).

Problems with Nameserverchange

In the current DNS-Setup a transfer from one nameserver operator to another is done very easily. With DNSSEC it is not possible to transfer the domain from one nameserver to another one without an outage (unless the old nameserver operator fully cooperates). The old nameserver operator has to give the private key for the zone to the new nameserver operator, or alternatively sign the zone with the new key. If he won't do the only chance to transfer the domain without outage is to unsign it, transfer it and sign it again – which is a time-consuming process.

DNSSEC is incompatible with some existing solutions

DNSSEC can cause problems with some existing solutions like dynamic updates, DNS-manipulation applications, special DNS-setups like split-dns and existing routers and firewalls without DNSSEC support. Using DNSSEC with dynamic updates is possible, but access to the private key for generating the signatures for the new or changed records is needed. Hardware with DNS- and without DNSSEC support can cause problems with the new DNSSEC-records they receive.

DNSSEC standardization is not fully completed yet

The technical standardization parts of DNSSEC are mostly complete, but for the organizational and administrative parts, standards are still missing. Each registry that wants to rollout DNSSEC has to create ways and processes how to handle key management, key rollover, and how to implement DNSSEC in the existing registry transactions (like domain transfer). These solutions can differ from the solutions from other registries and big registrars which have to work with a lot of registries would have to implement new processes for each registry.

3 Position of nic.at

Nic.at is well aware of the latest developments regarding DNSSEC, follows the standardization efforts closely, and runs several internal projects around this topic, including preparation of the registry system, the nameserver network, as well as evaluating strategies regarding key management, provisioning of keys between registrars and registry, legal implications etc.

However, the standpoint of nic.at is that an introduction of DNSSEC at this point in time would burden the ccTLD ecosystem with an amount of work that is in no relation to the security to be gained (especially since countries with DNSSEC implementations show extremely low adoption rates of well below 1%). Currently nic.at sees no customer demand for DNSSEC for .at. Deploying DNSSEC is a big expense for the registry as well as for the registrars and the nameserver operators. Experience from other registries, which have DNSSEC already deployed shows that customers have only very little interest in “more secure domains”. The demand is also small if DNSSEC domains are sold for the same price like the “normal” domains. The

additional security could not balance the additional complexity and possible new source of errors. Currently the basic conditions (Root zone signed, software support, standardization) for a stable deployment are not given. A stable DNS-System is too important for putting it at risk with a too hastily deployment of DNSSEC – especially when the industry is not prepared.

Deploying DNSSEC for .at will require nic.at to spend at least 300 man-days, which occur through customizing and extension of the current systems. The costs for new hardware will be on top. DNSSEC could be extremely resource intensive; the size of the zonefile can grow up by a factor of 10. This requires new and bigger hardware. Such a big zonefile can cause also problems during loading into memory; the bigger the zonefile the longer reloading takes.

Additionally to the costs on registry site, there will be also significant costs on the registrars and nameserver side. Deploying DNSSEC for .at as “island” (only the registry, without support from the registrars and nameserver operators) doesn’t increase the security level at all. In recent talks with registrars, the indication is that there is no interest in rolling out DNSSEC. The biggest problem for registrars is that the investment for a DNSSEC-rollout can’t be earned back by pricing hikes. Experience from countries where DNSSEC is already commercially deployed shows that customers won’t pay extra money for DNSSEC-secure domains. Even in countries like Sweden, where the .se registry sells DNSSEC-domains for the same price as “non DNSSEC”-domains, the demand for DNSSEC domains is very low (as of 07/2009: about 19000 signed domains out of 886000 registered domains - .se offers DNSSEC domains since 02/2007).

However an attack or another emergency where DNSSEC is the only solution can require a fast deployment of DNSSEC. For this case nic.at worked and continues to work on emergency plans to be ready for that case. Furthermore, if the demand is given, nic.at can develop a DNSSEC testbed for .at and its registrars. This gives registrars the chance to get experience with DNSSEC.

4 References

DNS and all extensions are standardised by the IETF as RFC. A good overview about all DNS relevant RFCs is available at <http://www.dns.net/dnsrd/rfc/>. Current developments can be followed in the IETF working groups “DNS Extensions” (<http://www.ietf.org/dyn/wg/charter/dnsxt-charter.html>) and “Domain Name System Operations” (<http://www.ietf.org/dyn/wg/charter/dnsop-charter.html>).