(/en/)

It's all about domains... with Klaus Darilion from nic.at

25.06.2021

What is DNS security and how can technology help protect a domain? Today Klaus Darilion (nic.at) replies to our questions to learn more about how to keep safe what we are most fond of: domains!

(/fileadmin/_processed_/8/6/csm_Interview_KD_Blogbild_ffa2b05100.png)

The internet offers a user-friendly environment thanks to the DNS (Domain Name System), a hierarchical and decentralized naming system that associates numerical information with domain names. It has been an essential component of the internet since 1985! Have you ever wondered how the operability and security of such an important and essential system are assured in the long run?

Within the domain industry (https://en.domainreport.global/) there are organizations and professionals who are committed to making DNS a sustainable and reliable system for all internet users. Klaus Darilion, Head of Operations together with the team at nic.at (https://www.nic.at/en) are one of them. In particular, they assure the stability and performance of .at, the Austrian ccTLD (/en/domains/at-domains/). With an academic background in Electrical Engineering and research experience in the field of packet-oriented voice communication and particularly with SIP, Klaus has been part of nic.at since 2004, working on network design, network security, VoIP, VoIP security, DNSSEC, and AnyCast DNS. Since the end of 2014, he is leading the nic.at Operation team. He is definitely the expert we needed today to talk about DNS security. Get ready to underpin some technical aspects of DNS security with us!

What does it mean to work on DNS security?

Securing the DNS is a broad area: it begins with the registration and ends with the actual domain data received by internet users. Security in the DNS means that nobody can manipulate this data and the information is available all the time without downtime.Those who register a domain usually manage this through a web portal (or API) of a registrar. Whoever gets credentials to access this portal can manipulate, transfer or delete the respective domains. That is why domain owners need to keep that information secure and use two-factor authentication when offered. Registrars also have to ensure that their portals do not have any vulnerabilities, which would allow attackers to exploit the portal and then manipulate every managed domain.

A further element is the domain name system itself. Name server software must be kept up-to-date to work around potential security issues in the protocol. Furthermore, the name server setup must be designed to have 100% uptime, using multiple name servers, having enough capacity to withstand high DNS query rates and DDoS mitigation is necessary. Unfortunately, DDoS attacks are today a daily business on the Internet.

(https://www.internetx.com/Two-factor)

Find out more about two-factor authentication (2FA) (https://www.internetx.com/en/news-detailview/two-factor-authentication-protect-your-accounts/) and how to secure your domains in AutoDNS.

DNS is an essential part of the internet: why is it still so vulnerable to attacks today?

DNS is an old protocol from the days where only "good" people used the internet. Since then, many attacks were discovered where invaders could spoof wrong data into the DNS, and hence they could reroute internet users to the wrong websites. And this, mostly with the intent to distribute malware or steal login information. Whenever such an attack was detected, the DNS protocol was fixed - if possible.

However, most of the DNS protocol cannot be changed without introducing incompatibilities, which would exclude old devices from the system. Hence, workarounds have been implemented to overcome those attacks. For example, DNS uses a 16-bit transaction ID that only allows 65,536 different IDs. Increasing the number of bits is not possible, as it would break the protocol. Thus, workarounds like random source ports and 0x20 encoding (mixed case) increased the effective transaction ID to 32+ bits. In addition, as DNS mostly uses the User Datagram Protocol (UDP) it is vulnerable to attacks based on IP fragmentation.

The “DNS Flag Day 2020 (https://dnsflagday.net/2020/)” created awareness around this matter and as a result, many DNS providers configured their name server to use smaller DNS responses to avoid IP fragmentation. Every discovered attack could be mitigated by implementing workarounds in the name server software.

(https://www.nic.at/en)

With DNSSEC those attacks could be discovered easier or would not be possible at all. How does DNSSEC work?

DNSSEC uses public-key cryptography to protect DNS responses against manipulation. When queried for a certain domain name, a DNSSEC enabled authoritative name server not only responds with the requested data but also signs the data with the domain's private key. A resolving name server uses the domain’s public key to verify the signature. To verify the public key, a chain of trust is used where the fingerprint of a public key is published in the domain's parent zone. For example, the fingerprint of the public key of the domain nodesecure.com is published and signed by the .com domain. Furthermore, the fingerprint of the public key of the .com domain is published and signed by the DNS root zone.

An attacker, which manages to forge DNS responses, cannot forge the signature. This means, while non-validating resolvers would not detect a forged response, a validating resolver would detect the forged response and ignore it. Today, all major DNS services like 8.8.8.8 and 1.1.1.1 have DNSSEC validation enabled, but many internet access providers do not have enabled DNSSEC validation on their resolving name servers.

Although DNSSEC is mature and stable, there are still some problems:

1. One is related to old firewalls and CPE (Customer Premise Equipment), i.e. DSL/cable modems. Those devices often have buggy DNS implementation, which fails if they need to process DNSSEC. Therefore, it might happen that internet users suddenly cannot receive emails from users behind those old devices, once they activate DNSSEC for their domains.

2. Another problem is key management. Whenever you apply cryptography you need to prepare for key rollovers. For example, if private keys leak or if there is a vulnerability in the used algorithm and the keys need to be changed. In such cases, the use of the new keys and the retirement of the old keys must follow a certain timing. Otherwise, the domain will fail DNSSEC validation. Those timing requirements are very complex and error-prone.

Nowadays, name server software like Bind or Knot help during key rollovers, but still the main problem remains human error.

(https://www.nic.at/en)

How does a registry like nic.at make sure that its registrants have a safe domain name?

Security features are certainly indispensable today. In general, changes for .at domains need to be signed by the domain holder to ensure they wish these changes on their domain. Security is a central topic for us as a registry, which is constantly developed further. As my colleague Katharina Hackl, Head of Customer Service suggests, nic.at offers various security features for .at domains (/en/domains/at-domains/):

Security Lock: This service protects domains against unauthorized transactions. With Security Lock, every change goes into pending status, which means that it is held up by the system, and must be explicitly checked and confirmed by the domain owner.

Anycast DNS: If the domain owner wants to protect the domain not only against unwanted transactions, nic.at also offers its RcodeZero DNS Anycast service. With more than 40 name servers distributed worldwide, we ensure that our clients' online services are always accessible and optimally available under the same IP address.

DNSSEC: It enables the domain owners to make sure the users end up on their website.

Registrar Lock: In addition, another service exclusively for registrars is currently being set up. Before a desired change on the .at domain, the registrar must remove the lock from the domain. As soon as all changes are done, the lock is set again. The benefit of this service is that it can be used for self-protection by registrars but can also be ordered by the domain owner.

Can automation technology help the DNS to be more secure?

Malfunction of DNS is often due to human errors, i.e. copy/paste mistakes during domain configuration or domain delegation. This happens in particular when internet users register a domain with registrar A, but manage DNS with provider B or on their own. When using the DNS service of the registrar, most of these errors can be avoided, as the registrar will use highly automated processes for the domain configuration. Even more when DNSSEC is used, automation is the key to success. The registrar has automated key management processes, which ensure compliance with timing requirements, and the registrar can automatically update the chain of trust with the parent domain, i.e. the TLD registry.

What are the most innovative techniques currently in use to keep the DNS safe?

Citing my colleague Alexander Mayrhofer, Head of R&D at nic.at, the DNS ecosystem needs safety protection in the following two parts:

One is the registration/namespace management ecosystem, where registries and registrars perform the allocation and configuration of domains. The key to security here is to protect domain names against unauthorized modifications or deletions, be it because of loss of credentials, social engineering, or breach on a system-wide level. We see more and more registrars adding two-factor authentication to their login portals; most end users are already comfortable with those technologies from their bank, or even their Gmail accounts. In addition, registries are adding options for additional verification such as Registrar Lock and Security Lock creating an additional layer of security.

The second part of the DNS industry is the resolution path – the actual look-up of information based on domain names. Here we have to consider authenticity and privacy as well. DNSSEC provides the authenticity of the information, and has been around for a while, so it is not “innovative” anymore. What would be innovative, though, is encapsulating that functionality away from the IT administrators but on the customer’s side. Something like what Let’s Encrypt did to the administration of certificates. On the privacy side, more and more DNS traffic between stub resolvers and recursors is being encrypted, and this will probably continue. It will eventually expand to the communication between recursors and authoritative servers. DNS over QUIC is an innovation that we all are watching closely.

Where do you see DNS in the next few years?

On the registration/namespace management side, in accordance with my colleague Alexander Mayrhofer we do not expect many changes compared to today. Registrars, as well as registries, might face additional requirements on validation and verification of customer data. For example, those proposed by the European Union's NIS-2 directive (https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union). There will eventually be the next round of new gTLDs, but we expect that it will be much quieter than the first round, with much more realistic expectations than during the 2012 round. On the resolution side, more and more traffic will be encrypted, and we will see new protocols and new pathways to resolution.

Nevertheless, we can firmly say DNS is here to stay – social networks rise and fall in popularity, but a domain name is the only human-readable identifier on the internet that is independent of the policy, popularity, and operation.

(https://www.internetx.com/SAD)

A series of flaws in the software stack has led to a revival of the classic DNS cache poisoning attack. Find out how the SAD DNS attack looks like and how to mitigate this threat in the DNS (https://www.internetx.com/en/news-detailview/sad-dns-a-revival-of-the-dns-cache-poisoning-attack/).

Social Media

- (https://www.facebook.com/InterNetX)
- (https://twitter.com/InterNetX)
- (https://plus.google.com/102479657851423343448)
- (https://www.youtube.com/user/InterNetXGmbH)
- (https://www.linkedin.com/company/internetx-gmbh)
- (https://www.xing.com/companies/internetxgmbh)

Author

Simone Catania

Global Content & Communications Manager

E-Mail: presse@internetx.com

Domains (/en/domains/)

Servers (/en/servers/)

SSL Certificates (/en/ssl-certificates/)

InterNetX (/en/about-us/)

Legal (/en/legal/imprint/)