Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-678-682

DNSSEC DEPLOYMENT AND CHALLENGES

Đorđe Antić
Singidunum University, Belgrade

Abstract:
DNS (Domain Name System) is an Internet system that provides translation between domain names and numerical IP addresses. As an answer to security threats, DNSSEC (DNS Security Extensions) has been developed to strengthen DNS, using public-key cryptography through digital signatures. However, Internet-wide deployment has been slow, due to system complexity and operational difficulties. This paper provides information on the technologies involved, deployment and challenges that have been encountered.

Key words:
DNS,
Security,
Cryptography,
DNSSEC.

INTRODUCTION

Domain Name System (DNS) is the standard mechanism for mapping hostnames to IP addresses. It is one of the essential and fundamental parts of the Internet, providing infrastructure for other Internet services. However, it was not designed with security in mind, which allowed different threats to emerge, most notably DNS cache poisoning. In order to secure DNS, security protocol based on public-key cryptography was developed – DNS Security Extensions (DNSSEC). DNSSEC uses asymmetric cryptography to create digital signatures of DNS data[4]. These signatures, verifiable by resolving clients, provide the system with origin authentication, data integrity and authenticated denial of existence. Since DNS is hierarchical in nature, DNSSEC had to follow this model, forming a chain of trust.

On the other hand, although almost a decade had passed since the DNSSEC standard was finalized (2005), the security system has not seen widespread deployment or use. Many factors contributed to the slow progress, such as complexity of implementation and maintenance, operational difficulties and political issues. Some crucial steps towards global deployment have been taken, such as signing of the DNS root. But, new set of challenges have been created for the system and current global level of deployment is still low.

BACKGROUND

DNS

DNS is a globally distributed database. It is deployed on name servers and links domain names with IP addresses and other data. DNS is hierarchical, organized in the structure of a tree, with the root domain on top, as shown in Fig. 1. The DNS tree is divided into zones (e.g. .com, .net, .org), with each zone being a section delegated to a single administrative authority. Each zone is maintained by multiple authoritative name servers, providing name resolution for all domain names contained within.

DNS data on name servers is organized in the form of Resource Records (RRs). RRs of the same name, class and type are grouped into Resource Record Set (RRSet). The NS (names of DNS servers) and A (IP addresses) types of RRs are the most important for establishing of DNS hierarchy and its operation.

Translation of names for end users starts with the client application sending a query through a local stub resolver. It is received by a local caching resolver, which performs all the steps of traversing the DNS hierarchy of authoritative name servers from the root zone, in order to obtain an answer.

The DNS, however, possesses various security vulnerabilities[2, 3]. The caching resolver, which performs the most of the work in each name resolving process, is one of the weakest links. Over the past years, methods have been found which allow injection of bogus information into the resolver's cache, most notable being the one described by Dan Kaminsky in 2008[1].

DNSSEC

DNSSEC was designed to provide secure transactions between resolvers and name servers. Introducing cryptographically signed data in the form of four new Resource Records[5], DNSSEC provides:

- Data integrity. Resolver can determine whether the answer has been modified during transmission.

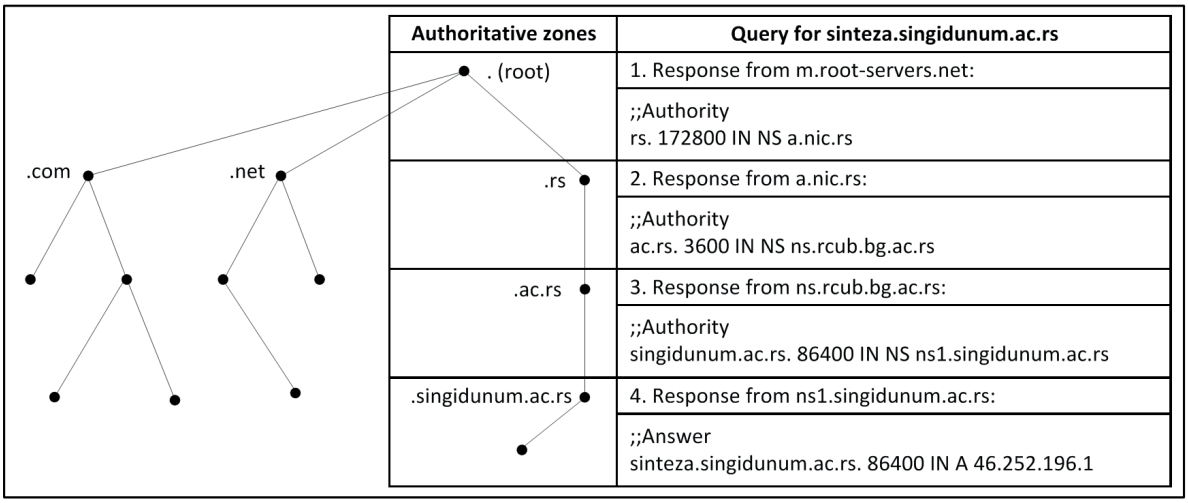

Fig. 1. DNS tree, authoritative zones and an example query

- Origin authentication of DNS data. Resolver can determine whether received answer comes from a given zone's authoritative name server.
- Authenticated denial of existence. Resolver can confirm that a given query is not resolvable.

Four new resource records are RRSIG (Resource Record Signature), DNSKEY (DNS Public Key), DS (Delegation Signer) and NSEC (Next Secure). DNSSEC name servers provide RRSIGs for various RRSets they hold. RRSIG is a digital signature created by hashing a RRSet and encrypting it with an administrator's private key for that zone. Matching public key is published in DNSKEY RR. After receiving a signed DNS response from a name server, DNSSEC resolver decrypts RRSIG with the zone's public key. Resolver then generates hash of the RRSet part of the response and compares it with hash received in RRSIG part of the answer. This mechanism verifies data integrity and provides origin authentication.

The DS RR is provided by every parent zone and represents point of delegation between parent and child zones which can be authenticated. It holds hash of the DNSKEY of the child zone for every parent zone. In order to verify DNSKEY of the child zone, resolver obtains relevant DS, RRSIG(DS) and DNSKEY from the parent zone. DS is verified by decrypting RRSIG(DS) and comparing the hashes, then used to authenticate DNSKEY of the child zone. In this manner, DS is used as a form of "certificate", being provided by parent zone and binding the child zone for its DNSKEY. Parent zone's name server thus becomes "trusted third party". These relationships form a chain of authentication that the resolver has to follow down the DNS tree from the root zone and its public key. The resolving process is illustrated in Fig. 2.

It is important to note that, in practice, two types of cryptographic keys are used per zone, Zone Signing Keys (ZSK) and Key Signing Keys (KSK). Secret ZSK is used to sign all data in a zone and its public counterpart is published in the form of DNSKEY RR. Public KSK is also published as a DNSKEY RR, but its secret part is used only for signing of DNSKEY RRs. Two types of keys are used for security reasons, because the more a key is used, the less secure it becomes. Since the ZSK is used to sign large amounts of data in DNS, and since every change to a zone requires the re-signing of the changed data, the data that is available for cryptanalysis is constantly growing. Therefore, ZSK's are changed (rotated), relatively often. If only one key was used, it would be necessary to send DNSKEY to the parent zone (to replace and re-sign DS RR) each time it was changed. To avoid this, separate set of keys is used and parent zone is contacted only when KSK is changed, which occurs less frequently.

Finally, authenticated denial of existence is provided by the NSEC RR. Its newest standard, NSEC3, is an improved version[8] which, through hashing of data, provides measures against zone enumeration.

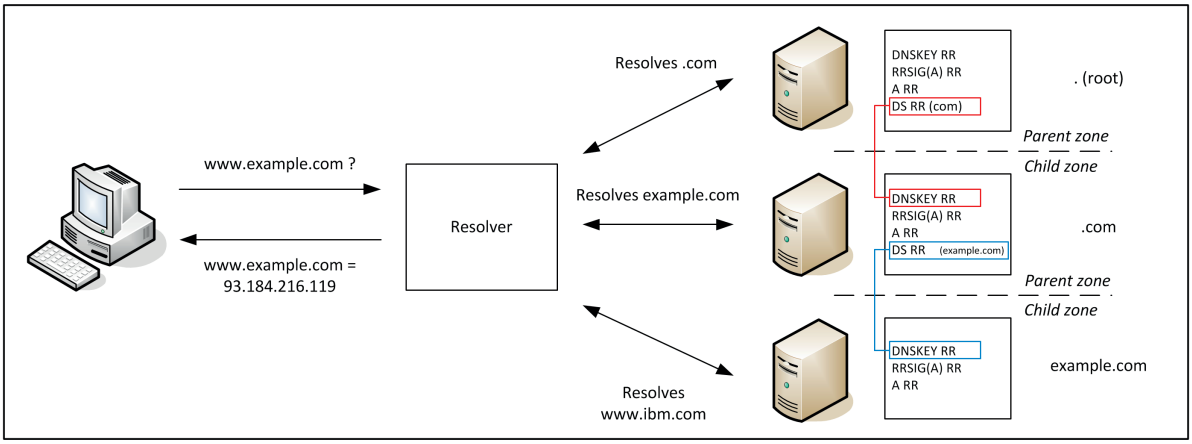

Fig. 2. DNSSEC resolving

DNSSEC DEPLOYMENT

Although DNSSEC as a standard was finalized in 2005, the deployment rate has been very slow, with signed root being deployed in July 2010. A study[19] in 2006. forecasted that the DNSSEC will suffer from bootstrapping problem, claiming the users "may only deploy when the network is in a state at which the immediate benefits of adopting the technology outweigh the costs." Since DNSSEC requires a minimal level of deployment before any users receive a benefit greater then their costs, deploying it has been difficult. According to National Institute of Standards and Technology (NIST) estimation[6] from March 2014, only 2% of global industry domains are DNSSEC enabled and operational, while universities are at 6% of operational DNSSEC domains. ICANN (Internet Corporation for Assigned Names and Numbers) research statistics[7] show that out of 482 Top Level Domains (TLDs) 292 have been signed until March 2014. Most of the deployment progress was made after ICANN published the root zone trust anchor and root operators began serving the signed root zone with keys in 2010.

Early adopters implemented pricing tactics to encourage DNSSEC adoption. In 2010, The Chech Republic's national Top-Level Domain (TLD) operator worked with largest registrars on signing all zones on their servers, free of charge. In 2013, more than 37% of .cz domains were secured with DNSSEC. Similar approach was used in Sweden, country that was the first to sign its TLD in 2005.

Before DNSSEC deployment, DNS management and maintenance was a task performed on demand and without strict time constraints. DNSSEC changed that, because it introduced concept of security policy. It became necessary to include various new elements for a successful DNSSEC deployment, such as:

- key generation and management procedures
- storage of private keys and their protection
- manner and frequency in which keys should be rolled over (scheduled and emergency)

Also, cryptographic standards had to be established:

- choice of cryptographic algorithm
- key length
- duration for the signatures to remain valid

All of these elements introduced tasks that placed new burdens on DNS administrators, usually without any best practice guides to follow. Also, first tools for generating key pairs and signing of zones (which should be performed with specific timing requirements) were complex and required significant work in the command line.

The tools have improved in time and new solutions, such as OpenDNSSEC, an international cooperation project, greatly facilitate the process. OpenDNSSEC is used by ICANN and several ccTLD (country code TLD) operators, including Sweden (.se), United Kingdom (.uk), Canada (.ca), France (.fr) and others. It secures zone data by adding digital signatures and other DNSSEC data prior to its publishing in an authoritative name server for that zone, as shown in Fig. 3. All cryptographic keys are stored in a security module in conformance with PKCS#11 (Public-Key Cryptography Standards) interface. The purpose of this module, among others, is to generate cryptographic keys and sign information without revealing private key material, as recommended in IETF "DNSSEC Operational Practices" document[24]. A choice of either a hardware device (HSM, smartcard or token) or a software implementation (softHSM) is available, depending on security requirements and investment constraints.

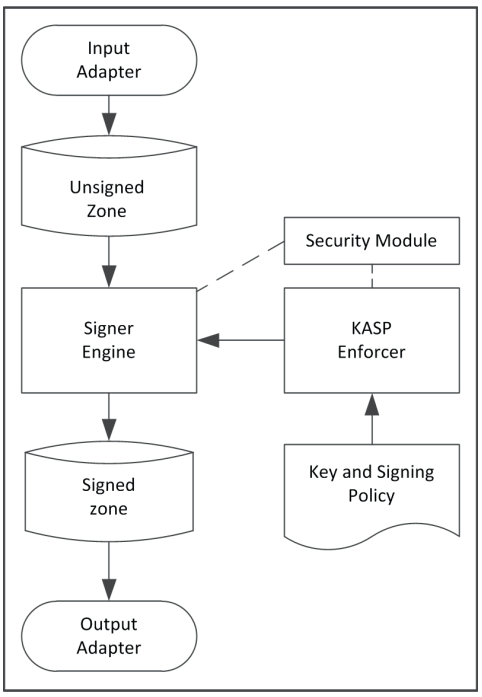

Fig. 3. OpenDNSSEC operation

DNSSEC CHALLENGES

Packet size issues

The specification of DNS mandates that, using UDP protocol, the largest size a DNS response could have cannot exceed 512 bytes. In the case 512 bytes are not enough, rule is to use TCP and establish a full TCP connection. This causes significant network traffic overhead. To remedy the problem, EDNS0 standard was introduced[18], allowing the use of larger DNS responses in UDP protocol. However, this standard came into conflict with generally established firewall rules and practices.

It has been an established practice not to allow DNS responses larger than 512 bytes through the firewall. This is a part of practice that blocks all packets deviating from the original specifications and many firewalls default to this practice. Thus it became necessary to manually disable these restrictions.

With larger packet sizes, usually up to 4096 bytes, came another issue, pertaining typical maximum frame size of ethernet (1500 bytes) and other protocols. What happens is that the large packet becomes fragmented, divided into several smaller packets. Fragmented packets are considered to pose a certain security threat, as they can be used to encapsulate or obfuscate malicious data. Thus, another established firewall rule came to attention,

blocking fragmented UDP packets by default. The solution was either to allow UDP DNS fragments, configure firewalls to reassemble the fragmented packets and then apply traffic rules, or to limit maximum packet size on name servers[21].

Introduction of large packet size with EDNS0 also made a well known malicious technique called DNS amplification much more effective. Attacker can send DNS query with spoofed source address, and the response will be sent to victim's IP address. DNSSEC data makes these responses fairly large, increasing the effectiveness of the attack. In a scenario with attacker using botnets, the amount of traffic that can be sent to a victim can be substantial[20].

Enumeration of zones

The NSEC Resource Record presented a new vulnerability – exposure of information that are usually private. Although introduced in order to enable authenticated denial of existence (confirming that a domain does not exist), it also created a potential for enumeration of zones (i.e. zone walking). NSEC RR spans a gap between two names in a zone by pointing to the next domain name. Following these pointers, a zone could be traversed from one end to the other and every record could be discovered. Since DNSSEC must be able to report when a domain is not found, solution was implemented in 2008. with a new version of the standard, NSEC3. Instead of the name of the next domain in a zone, the record holds only its cryptographic hash (with multiple iterations and an optional salt, to deter dictionary attacks).

DS Resource Record issue

There is no mechanism for automatic creation or update of the relationship between a zone secured with DNSSEC and its parent. The only way to create it is to communicate with the parent zone manually, every time KSK is changed, at least once every year. This can be a pitfall, since failure to communicate the change in timely fashion can lead to zones failing DNSSEC validation. Current standard for relaying this information to parent zone is through DNS Security Extension Mapping for the Extensible Provisioning Protocol[23], a protocol used for allocating objects within Internet registries. These mappings provide interfaces for submission of DS or key data information for a domain name. Information received can then be extracted and used to publish DS RR, but the described mechanism is reliant on zone administrator submitting the necessary data.

Governance issues

Alongside technical challenges, deployment of DNSSEC has suffered due to the political implications. ICANN, as a body coordinating key technical services critical to DNS, has contractual ties to United States Government. The U.S. Department of Commerce (DoC), although not playing any role in internal governance or day-to-day operations of ICANN, holds three contractual agreements related to DNS:

- The Affirmation of Commitments between DoC and ICANN[9],
- contract between IANA/ICANN and DoC to perform various technical functions such as editing the root zone file[10] and
- the cooperative agreement between DoC and Verisign to manage and maintain the official DNS root zone file[11].

The Verisign/DoC agreement also provides that the DoC retains policy authority and that Verisign "shall request written direction from an authorized USG (Department of Commerce) official before making or rejecting any modifications, additions or deletions to the root zone file" [12].

The described relationship between U.S. Government and ICANN has long been a source of international discontent. In 2005, DoC's National Telecommunications and Information Administration (NTIA) released a statement[14] in which it was announced that "The United States Government intends to preserve the security and stability of the Internet's Domain Name and Addressing System […] and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file" This statement was released shortly before a United Nations multistakeholder Working group on Internet Governance (WGIG), with members from various countries and interest groups (governments, private sector, academic sector, civil society organizations) published its report[13] in which it was stated that "no single Government should have a pre-eminent role in relation to international Internet governance". According to a former member of ICANN's Generic Names Supporting Organization (GNSO), which represents the non-commercial users[15], "ICANN works as a service concessionaire ("incumbent") subject to regulation by the U.S. Federal Government - as is the relationship between a telecommunications company and the FCC." Also, a 2013. Congressional Research Service Report[16] states that "U.S. Government maintains instruments that provide a level of control or oversight over ICANN functions."

Having this in mind, it should not come as a surprise that concerns were raised pertaining DNSSEC deployment, as the content of the root zone is a politically important and sensitive matter. Phillip Hallam-Baker, internationally recognized computer security specialist, wrote on implications of root signing on the Internet Engineering Task Force (IETF) mailing list[17]: "Consider that this is an infrastructure which needs to be robust over a timescale of several decades if not centuries. Consider also the likelihood that whoever is in charge of the root might perform an action that some party might consider a defection over such an extended timescale.[…]The parties have authority but not power. If the root is signed by a unitary entity, that entity has absolute power. A defection cannot be countered by a fracture of the root. Today scope for defection is kept in balance by the lack of security. The root is ultimately defined by the location to which a particular network provider directs UDP packets with the

root server IP address. After signing, the root will be defined by the knowledge of the private key corresponding to the widely distributed embedded public key.[…] The idea that control of the DNS root will not be subjected to even more considerable geo-political pressure is naive. In 1995 deployment could have taken place without attracting undue attention, that is not the case today."

In an announcement[22] from March 2014, NTIA stated "its intent to transition key Internet domain name functions to the global multistakeholder community" and tasked ICANN with developing a transition proposal. This announcement has attracted significant community attention and could represent a turning point in Internet governance. However, it remains to be seen what this transition will bring in practice.

CONCLUSION

DNSSEC has come a long way since the first Request for Comment (RFC) was published in 1997. Although the protocol was finalized in 2005, initial deployment was slow, due to technical obstacles, requiring subsequent modifications and additions. However, cryptographic technology has been a factor which made the protocol complex to implement, further delaying widespread adoption. Also, being applied on an Internet-scale, DNSSEC has global political implications concerning signing of root, which came to light as a significant focal point of attention. Experience gained so far from DNSSEC implementation and deployment will help future work in overcoming the challenges faced with securing DNS and hopefully serve the global community in building a safer Internet.

REFERENCES

[1] S. Friedl, "An Illustrated Guide to the Kaminsky DNS Vulnerability" – http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, 2008.

[2] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC", Proceedings of The Second International Conference on Availability, Reliability and Security, pp. 335-342, April 2007.

[3] D. Atkins and R. Austein, "Threat analysis of the domain name system (DNS)", RFC 3833, Internet Engineering Task Force, Aug. 2004.

[4] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "DNS Security Introduction and Requirements", RFC 4033, Internet Engineering Task Force, March 2005.

[5] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, Internet Engineering Task Force, March 2005.

[6] "Estimating IPv6 & DNSSEC Deployment SnapShots" – http://fedv6-deployment.antd.nist.gov/snap-all.html, National Institute of Science and Technology, March 2014.

[7] "TLD DNSSEC Report" – http://stats.research.icann.org/dns/tld_report/, Internet Corporation for Assigned Names and Numbers, March 2014.

[8] B. Laurie, G. Sisson, R. Arends, D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, Internet Engineering Task Force, March 2008.

[9] "Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers" – http://www.ntia.doc.gov/files/ntia/publications/affirmation_of_commitments_2009.pdf, September 2009.

[10] http://www.icann.org/en/about/agreements/iana/contract-01oct12-en.pdf, October 2012.

[11] http://www.ntia.doc.gov/legacy/ntiahome/domainname/nsi.htm

[12] http://www.ntia.doc.gov/legacy/ntiahome/domainname/agreements/Amend11_052206.pdf

[13] "Report of the Working Group on Internet Governance", http://www.wgig.org/docs/WGIGREPORT.pdf

[14] "U.S. Principles on the Internet's Domain Name and Addressing System", National Telecommunications and Information Administration", June 2005, http://www.ntia.doc.gov/files/ntia/publications/usdnsprinciples_06302005.pdf

[15] C. Alfonso, "Word Matters", January 2006, http://vecam.org/article533.html

[16] L.G. Kruger, "Internet Domain Names: Background and Policy Issues" – https://www.fas.org/sgp/crs/misc/97-868.pdf, Congressional Research Service, December 2013.

[17] H.B. Phillip, "RE: Last Call comment on draft-weiler-dnssec-dlv-iana-00.txt", August 2007, http://www.ietf.org/mail-archive/web/ietf/current/msg47560.html

[18] J. Damass, M. Graff, P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", RFC 6891, Internet Engineering Task Force, April 2013.

[19] A. Ozment, S.E. Schechter, "Bootstrapping the Adoption of Internet Security Protocols", The Fifth Workshop on the Economics of Information Security, June 2006.

[20] T. Rozekrans, J. de Koning, "Defending against DNS reflection amplification attacks", University of Amsterdam, February 2013.

[21] G. van den Broek, R. van Rijswijk, "Recommendations for dealing with fragmentation in DNS(SEC)", RIPE NCC, 2012.

[22] "NTIA Announces Intent to Transition Key Internet Domain Name Functions", National Telecommunications and Information Administration, March 2014, http://www.ntia.doc.gov/print/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

[23] J. Gould, S. Hollenbeck, "Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)", RFC 5910, Internet Engineering Task Force, May 2010.

[24] O. Kolkman, W. Mekking, R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, Internet Engineering Task Force, December 2012.