Rena T. Gasimova
Institute of Information Technology of ANAS, Baku, Azerbaijan
rena.gasimova@science.az

DOI: 10.25045/jpit.v06.i2.06

SECURITY OF GLOBAL DOMAIN INFRASTRUCTURE IN THE INTERNET

DNSSEC technology is used in preventing DNS search result hacks, eliminating falsifications and ensuring security of domain name systems. The article analyses attacks undertaken to DNS server and justifies the necessity of DNSSEC technology application. The article researches the present state and problems in implementation of DNSSEC technology, advantages and scope of solvency in ensuring the security of DNS systems. Recommendations for realization of these technologies are proposed.

Keywords: *domain names system, DNS server, information security, E-signature, registrar, top level domains, Crypto Officer*.

Introduction

A pressing task for states is the struggle for the right to control their own information environments, which encompasses the protection of economic, political, cultural, national, spiritual and military values. Integral factors in the transition to an information society are the improvement of governance and ensuring its transparency, the creation of national information resources, protection of national interests and values in the virtual space, development of a knowledge-based economy, introduction of a wide range of new technologies, information security and the protection of freedom and integration into the global information space. The Internet offers new opportunities for the development of all areas of human activity: science, education, politics, business and manufacturing. The Internet can shape the public’s views in addition to political, economic and military decision-making.

Active use of the Internet for information warfare is explained by its domination over traditional methods (mass media) and technologies. Research shows that the crucial problems across the Internet are the prevention of the use of information resources and technologies used for crime and terrorism; protection of intellectual property, human rights, trade rights and domain names; and ensuring national security and data privacy [1].

The Internet has become a medium of communication and global commercial business with over three billion Internet users. Internet addresses are managed through the Domain Name System(DNS). Today, DNS is the largest distributed database, processing billions of requests daily. Thirteen root servers ensure DNS’s operation on the Internet, and they are owned by the Internet Corporation for Assigned Names and Numbers (ICANN). Of the servers, 10 are in the US, one is in Japan, one is in the Netherlands, and one is in Sweden. In 2012, the L-root DNS mirror root was launched in Azerbaijan [2-5]. Studies have shown that most research has focussed on identifying DNS security problems. This research has identified ways to prevent DNS server overload and methods of attacking DNS and modern defence technologies. A review of the scientific and technical literature shows that no effective measures have been taken to handle false responses of DNS. Domain Name System Security Extensions (DNSSEC) are one of the methods to prevent falsification [6-10]. DNSSEC is the DNS protocol extension that minimises attacks in which DNS addresses change. Other research has demonstrated the suitability of using cryptographic mechanisms (electronic signatures), which is the standard approach of modern security systems to protect DNS data, and these studies provide statistics on the most commonly used methods of attacks. However, in terms of the execution, some unresolved problems of DNSSEC still remain. The analyses show that registration and management problems in the use of DNSSEC have not been resolved yet [11-13].

Emergence of DNSSEC technology

DNSSEC security certificates were first offered by the Internet Engineering Task Force (IETF) to provide necessary protection, and they focus on responding to DNS requests of DNS clients and ensuring their integrity using open key cryptography. Data access and requests' confidentiality are not provided. Ensuring DNS security is of great importance for Internet security as a whole [14]. Studies show that a DNS problem is its vulnerability to all kinds of attacks, which affects its availability and integrity. Malefactors send requests to the servers with wrong characters to access passwords, credit card numbers and other confidential data. As the address appears on the bar at the top of the browser, and the website is as expected by the users, they are often unaware that the request has been directed elsewhere and they are oriented to phishing sites and fake Internet banking. DNSSEC was developed to protect clients from fake DNS data through a digital signature. When verifying the signature, the DNS client checks the accuracy and integrity of the data. DNSSEC is compatible with the current DNS system and earlier versions of the programs, and does not encode the data or change its control. DNSSEC can verify general-purpose cryptographic data stored in DNS. DNSSEC does not provide confidentiality of the data, that is, all DNSSEC responses are authenticated, but not encoded. Other standards are used to supply large volumes of data sent through the DNS servers. DNSSEC specifications describe current DNSSEC protocol in detail [15]. Studies show that when the DNS was established, the system did not have mechanisms to protect the response of the server from information changes. DNS protocol was developed not for security purposes, but for the creation of scalable and distributed systems.

In this case, the clients verified received information using2byte identifiers requiring malefactors to examine the value of 65536 to delete the cache. This means that DNS data is intentionally or accidentally damaged, and the DNS-server caches them to optimise the speed, and sends inauthentic data to the "clients". In 1990, Bellovin revealed serious safety shortcomings and published a report on this issue in 1995. Studies in this field increased after the publication of the report in 1995 [16, 17]. The first edition of DNSSEC was published as the RFC 2065 (Request for Comments) IETF in 1997. Attempts to perform the specification gave a rise to the emergence of a new RFC 2535 63 specification in 1999. The DNSSEC was projected based on IETF RFC 2535. Unfortunately, the IETF RFC 2535 specification had a serious problem in terms of Internet scalability. In 2001, it became clear that this specification was not appropriate for large networks. DNS servers were not often simultaneous with top-level domains (parents), but non-simultaneous, connected DNSSEC data could cause Denial of Service (DoS). DNSSEC was more capacious than traditional DNS in terms of computing resources. The first DNSSEC version required communications containing large-scale data to change successors (DNS zones of the successor are transferred to the parent completely and the parent makes changes and returns it to the successor again).. In addition, changes in the common key can cause a catastrophic effect. For example, if the COM zone changes its key, 25 million texts must be sent, and thus all the successors must update the texts. Therefore, DNSSEC RFC 2535 specifications could not be scaled to the Internet. These problems and major changes in DNSSEC have given rise to the new specifications (RFC 4033, RFC 4034 and RFC 4035). New versions removed the chief problem of the previous ones. Even though the new specifications require additional work to verify the key, they were suitable for practical applications. In 2005 the current version of DNSSEC was developed.

Signature of the root zone. For a full verification of the data received with the help of DNSSEC, a trust chain received from the root zone DNS (.) is required. The implementation of a correctly signed root zone in DNS servers could cause the collapse of the Internet. Therefore, IETF worked out the gradual introduction procedure of the distribution mechanism of the keys and root zones signatures with ICANN. The procedure lasted eight months and included step-by-step introduction of previous unreliable root zones in DNS servers. This step was needed to ensure server loading tests, to maintain compatibility with older software and to gain the possibility of returning to the previous configuration. In 2005, the DNSSEC protocol was first demonstrated in the Sweden (.SE) zone. In 2007, Brazil (.BR), Bulgaria (.BG), and in 2008, the Czech Republic (.CZ) were added. In 2009, the first top-level domain (TLD) in the zone for organisations (.org) that supports security protocol was used. On May 5, 2010, all DNSSEC domain names were fully applied in the 13 root servers. By June 2010, all root servers worked in the zone signed with an invalid key. In July, ICANN held an international conference on the generation of root-zone signing keys. On July 15, 2010, the root zone was signed and began to be applied on servers. On July 28, ICANN announced the completion of the application process. The root zone was signed with an electronic signature and distributed throughout the DNS system. On March 31, 2011, the largest zone, COM, signed with an electronic signature. By 2011, the number of the zones supporting TLD reached 59 and 90 in 2012. The US government shifted all government (.gov) domains to the protocol. According to ICANN, by April 10, 2015, 726 top-level domains out of 897 supported DNSSEC [18-21] and the national registrars in DNSSEC implementation were more active. Subsequently, according to statistical report of SIDN for the year 2014, the Dutch national domain NL led the list of top-level national domains for supporting DNSSEC protocol. In the Netherlands 5.4 million domains are registered; 1.7 million of them support DNSSEC protocol. According to the statistics, the Czech Republic domain CZ is ranked second for supporting DNSSEC protocol. More than 1.2 million domains were registered in the CZ zone; 450 of them support the protocol. In December 2013, the Czech government adopted a resolution to ensure the development of a safe protocol. The resolution forced all websites of public authorities to support DNSSEC by the end of June 2015. According to the CZ administrators, it was a successful step taken by the government to ensure the development of a safe protocol [22, 23]. The top ten countries supporting DNSSEC included Brazilian BR (12.6%), Sweden SE (8.7%), the European Union EU (6.2%), and the domains of .com (8.4%), .net (1.8%) and .org (0.9%) (See Figure 1). In 2011, the Russian Federation decided to introduce DNSSEC in the SU zone and to study the experience of other countries. Implementation of DNSSEC in the SU zone had three goals: to allow interested users to use the protocol, to lay the basis for experiments, and to draw attention to the new technology. In early 2012, the Russian РФ and RU signed the application of DNSSEC protocol. Currently, DNSSEC protocol has been signed in 300 domains of the RU zone, and about 40 of the РФ zone [24].

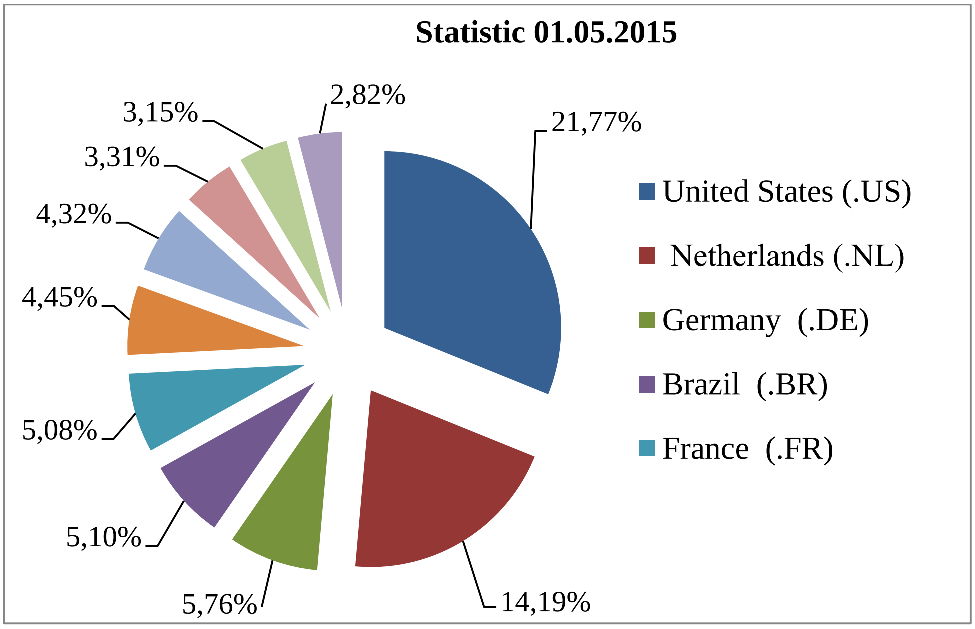

Figure 1. Top ten domain zones supporting DNSSEC technology.

Infrastructure of the keys. ICANN selected a model for the signature zone control that was controlled by Trusted Community Representatives (TCR) selected from those who are not part of DNS root zone management. Elected representatives are appointed as crypto officers (CO) and recovery key shareholders (RKSH). The CO is presented with a physical key, which activates the generation of zone signing keys (ZSK). The RKSH owns a smartcard containing a key signing key (KSK) used with cryptographic equipment.

In accordance with ICANN's procedures, the CO participates in ZSK generation up to four times per year, while RKSH participates only when the CO loses the keys, or when the root zone is exposed to risk.

DNSCEC opportunities and challenges

Zone signing alone is not sufficient; the registrars, providers and customers have to use it. The key problem is to deliver the “trust chain” to the end user. Accredited registrars are actively engaged in this process. The introduction of DNSSEC can be delayed for the following reasons:

- DNS servers and clients must support DNSSEC;
- Disagreement among the major actors for the ownership of top-level domains (.com, .net);
- Updated DNS-resolvers operating with DNSSEC must use TCP;
- Each client must have a confidential public key before using DNSSEC;
- Increase in network load due to a significant increase in request traffic (6-7 times);
- Overload of server processors due to the generation and verification of signatures on demand (in this case, DNS servers may need to be replaced);
- Increased requirements for data storage because the signed data require a large capacity;
- The software of server and client components must be developed, tested and added (requiring time on the Internet);
- Sharp increase in the risk of DNS amplification attacks.

Most of the technical problems have been resolved by the Internet development community. Maximum DNSSEC efficiency can be achieved by the distribution of the system from the high level of the Internet hierarchy (root zones and top-level domains) to the individual domain names. Registries, registrars, registration owners, hardware and software manufacturers, hosting companies, government agencies, technical services, and the Internet community are responsible for successful implementation. The application of DNSSEC offers clients, registrars and providers new opportunities to:

- protect brands and clients;
- reduce risks;
- strengthen the clients’ trust and reliability;
- strengthen the domain names owners’ trust and loyalty;
- provide extra protection of the network;
- attract and maintain the clients interested in providing security;
- protect the company's performance;
- develop and offer new services (e.g., signing the zone for the domain name owner);
- secure the company's reputation by applying advanced methods of ensuring Internet security and by caring about the clients’ protection.

The implementation of DNSSEC ensures that the providers can protect clients, consolidate the reputation of the leaders to provide security for Internet users and guarantee good conditions for successful competition. Thus, the introduction of DNSSEC technology is designed to address the following issues:

- to extend the protection capabilities of DNS;
- to prevent attacks against DNS;

- to ensure the integrity of DNS;
- to ensure extra protection of trademarks and clients;
- to protect against cybercriminals;
- to prevent website or email users from entering their credit card data or passwords on phishing sites;
- to provide a certain level of protection for the organisation;
- to use advanced protection technology.

Conclusion

The rapid introduction of DNSSEC technology can be attributed to favourable economic conditions, the need for Internet security, and ease of use. The clients, registrars and providers taking advantage of the technology can have significant impact on the development of the products and services, supporting and strengthening the businesses of the user. Thus, high-level security and reliability are guaranteed by applying DNSSEC to prevent certain types of attacks and redirecting. In addition, innovation opportunities, which increase the reliability and data integrity for web certificates (SSL/TLS) can be ensured. DNSSEC addresses information security issues by identifying the responses to the requests on the network and verifying their integrity. DNSSEC analyses show that national registrars are more active in its application, though some problems still remain, indicating that top-level domain zone registrars must work on the implementation of DNSSEC. Thus, the relevant government agencies must take certain measures to ensure the development of a secure protocol, and the process must meet international norms and national legislation.

References

1. Gasimova R.T., Problems of Internet domains and their solutions. Baku: ANAS “Information Technologies” Publishing House, 2012, 164 p.
2. Alguliyev R.M., R.T.Gasimova//Developing intelligent analysis system of domain names. Problems of Information Technology, 2011, No 1, 29-36 pp.
3. www.internetworldstats.com/stats.htm
4. Gasimova R.T., www.internetworldstats.com/stats.htm // Comparative analysis of geographical top-level domains of the Internet. Information Technology, 2011, No 7, 18-23 pp.
5. Alguliev R.M., Gasimova R.T. Identification of Categorical Registration Data of Domain Names in Data Warehouse Construction Task // Journal Intelligent Control and Automation, USA, 2013, vol.4, no.2, pp.227–234.
6. Imamverdiyev Y.N. Analysis of the current state of researches on the management of E-government information security problems// Problems of Information Society, 2012, No 2, 19-26 pp.
7. Imamverdiyev Y.N. Conceptual model for E-government information security management//Problems of Information Society, 2013, No 1, 53-58 pp.
8. Massey D., Denning D.E. Guest Editors' Introduction: Securing the Domain Name System // IEEE Security and Privacy, 2009, vol.7, no.5, pp.11–13.
9. Guanchen Chen, Matthew F. Johnson, Pavan R. Marupally, Naveen K. Singireddy, Xin Yin, Vamsi Paruchuri. Combating Typo-Squatting for Safer Browsing / WAINA '09 Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops/ Bradford, United Kingdom, 2009, pp.31–36.
10. Pappas V., Massey D., Zhang L. Enhancing DNS Resilience against Denial of Service Attacks / Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Edinburgh, 2007, pp. 450–459.

11. Ariyapperuma S., Mitchell C.J. Security Vulnerabilities in DNS and DNSSEC / Proceedings of the Second International Conference on Availability, Reliability and Security, Vienna, 2007, pp. 335–342.
12. Chandramouli R., Rose S. Open issues in secure DNS deployment //IEEE Security and Privacy, 2009, vol.7, no.5, pp. 29–35.
13. Osterweil E., Zhang L. Inter-administrative challenges in managing DNSKEYs // IEEE Security and Privacy, 2009, vol.7, no.5, pp.44–51.
14. Mamaev M.A., Petrenko S.K. Technologies to protect information on the Internet, SPb.: Peter, 2002, 243 p.
15. Radivilova T.A., Bushmanov V.S. Analysis of the main attacks on DNS-server, and methods of use of DNSSEC in the DNS-server protection // Technological audit and production reserves, 2013, No 1 (10), Volume 2, pp.16-19.
16. Carl Landwehr, Dan Boneh, John Mitchell, Steven M. Bellovin, Susan Landau, Mike Lesk. Privacy and Cybersecurity: The Next 100 Years / Proceedings of the IEEE, PP(99):1–15, May 13th, 2012, vol.100, pp.1659–1673.
17. Steve Bellovin. Using the Domain Name System for System Break-Ins / SSYM'95 Proceedings of the 5th conference on USENIX UNIX Security Symposium, 1995, USENIX Association Berkeley, CA, USA, vol.5, pp.18–28.
18. Metzger P., Simpson W.A., Vixie P. Improving TCP security with robust cookies / Proceedings of the 26th Large Installation System Administration Conference (LISA‘12), 2009, vol.34, № 6, pp.86–97.
19. Ballani H., Francis P. Mitigating DNS DoS Attacks / Proceedings of the 15th Conference on Computer and Communications Security, Virginia, 2008, pp.189–198.
20. Arends R.L., Austein R.U. DNS Security Introduction and Requirement // RFC 4033, 2005, 47 p.
21. www.root-d nssec.org/
22. www.dnssec.cz/
23. www.sidn.nl/annualreport/dot
24. http://stats.research.icann.org/dns/tld_report/