Bulletin of the *Transilvania* University of Braşov • Vol 10(59), No. 1 - 2017
Series III: Mathematics, Informatics, Physics, 193-202

SECURITY CHALLENGES OF .RO DOMAINS AT THE CORE OF INFORMATION SOCIETY

Doina BANCIU[1], **Ionuţ PETRE**[*2] **and Ionuţ SANDU**[3]

Abstract

As the Information Society is not only surrounding us, but also evolving rapidly, there is a need for keeping up the pace with the evolution. The .RO domains are an important part of what constitutes the information society in Romania. The Romanian Top Level Domain is always facing attacks, and there are measures that must be implemented continuously and security developments that are performed to maintain the proper functioning of the Internet in the country. The system comprises several dedicated applications for the management of .RO domains, and their development and security represents a continuous project.

2000 *Mathematics Subject Classification:* 94A99, 68M11
Key words: information society, .RO domains, web domains security, internet security

1 Introduction

It has been only a matter of decades for the information society to make the leap from a vague term that attempted to define the future of mankind to a reality that surrounds the globe. In a short period in history, the world made a significant progress in the information technology and communication. Most of the current devices – computers, TVs, home appliances or vehicles wear the mark of technology and are meant to offer smart services for the citizens. The Internet evolution is related to the technological advances, but in the same way it is about the social factors that are creating new consequences for the society.

[1] University of Bucharest, The Academy of Romanian Scientists

[2] ∗*Corresponding author*, ICI Bucharest - National Institute for Research and Development in Informatics, RoTLD - Romania Top Level Domain, e-mail: ipetre@ici.ro

[3] ICI Bucharest - National Institute for Research and Development in Informatics, RoTLD - Romania Top Level Domain, e-mail: ionut@rotld.ro

2 Information Society

It is difficult to define a concept of information society that englobes all its characteristics. In a wider accepted manner, it can be defined as the society that is dominated by the production and consumption of information based on ITC in economic, social, cultural and political life. It represents a new evolutionary stage that brings superior lifestyle and involves the intense use of information in every aspect of our existence. It allows the broad access to information, introduces new ways of knowledge management and enhances the economic globalization.

The information society has its beginnings in the period of 1960, even though at that time the discussion was mostly about the informatics world. The information society as we know it today has really emerged with the Internet. This has been not only a technological phenomenon but also a social factor, with the participation of the ever-increasing number of users that led to its current spread. As ***Alvin Toffler*** said in his book, ***The third wave***, "*It's the computer-but it's not just the computer. It's the biological revolution-but it's not just the biological revolution. It's the shift in energy forms. It's the new geopolitical balance in the world. It's the revolt against patriarchy. It's credit cards plus video games plus stereo plus Walkman units. It's localism plus globalism. It's smart typewriters and information workers and electronic banking. At one end, it's the space shuttle-at the other, it's the search for individual identity. It's flex-time and robots and the rising militancy of black and brown and yellow people on the planet. Above all, it's the acceleration of change, itself, which marks our moment in history.*" [11]

The innovation in ICT has transformed national, regional, and local economies at an unprecedented pace. The implementation of the Digital Agenda for Europe and the completion of the Digital Single Market imply the evolution of business models and the generation of both positive and negative externalities that need to be appropriately managed to maximize the benefits and minimize the unfavorable effects [9].

Given the potential for additional growth this represents, a more thriving EU services sector is a priority for the European Commission, as services are the driving force of the EU economy and statistics show that around nine out of ten new jobs are created in this sector [1]. Improved access to ICT has contributed to a narrowing of the gap in average incomes between countries while increasing inequality within countries and among individuals. New jobs that appeared as a result of ICT evolution have lifted many individuals with low income from undeveloped countries [2].

3 Internet Domain Names

The web as we know and use today functions as WWW - World Wide Web – is the global information medium that is used for communication over the Internet has its beginning in 1991, when Tim Berners-Lee established the basis of HTTP protocol and web servers while working for CERN.

The activities in the on-line environment are initiated using requests to the Domain name system, which is responsible for three major facts: the *unique name and number identifiers* of the on-line resources and the *distributed technological system* which comprises servers, databases, nodes, transport protocols and the *governing institutions* that administrate the domain name system. [3]

The DNS makes the Internet accessible to humans. The main way computers that make up the Internet find one another is through a series of numbers, with each number (called an "IP address") correlating to a different device. For the human mind it is challenging to remember long lists of numbers so the DNS links a precise series of letters (and/or numbers) with a precise series of numbers (the IP address) [12]. This also presents the advantage that domains are not restricted to use a certain computer, and the host servers can be easily modified.

Initially, domain names were seen only as a technical resource that simplifies the use of Internet. Over the years, with the vast expansion of the Internet towards commercial services, the domain names have gained importance. This fact is demonstrated by the exponential growth in the number of domain names per country, and by the number of generic domains.

For the proper functioning of the internet domain names the allocation of the unique resources – domain names, IPs, autonomous system numbers, protocol numbers, ports – is performed in a centralized manner. The global authority that is responsible and supervises this operation is IANA – Internet Assignment Numbers Authority, a department of the higher-level organization ICANN - Internet Corporation for Assigned Names and Numbers.

ICANN is responsible for the management of the *gTLD – generic Top Level Domain* and for the systems of national domain names *ccTLD – country code Top Level Domain.*

Country-codes can be seen as Internet infrastructure spaces with circumscribed geographical boundaries embedding different legal and cultural contexts [3]. The ICANN governance on the national systems has been in a total support of autonomy, even though there have been few attempts in order to re-delegate the ccTLDs. The official position was "ICANN does not have the unilateral power or authority to re-delegate the ccTLDS, and doing so would interfere with contractual relationships" (ICANN, 2014).

4 Romania - from isolation to WWW

Romania suffered from a big technological gap, as in the period of 1980-1989, the exchange on technical-scientific information was extremely difficult as the public institutions were forbidden to make subscriptions to the foreign R&D journals.

It was only in December 1992 when the first on-line connection was established between ICI ad the Vienna University, using the TCP/IP protocol. The .RO domain became operational in Romania on February 26, 1993, with the telnet, ftp, gopher, wais, netfind and www protocols.

According to the data published by the National Institute of Statistics, in 2016 in Romania 65% of the houses are connected to the internet network. Regarding the population, 69.7% of people aged 16-74 years have used the Internet in 2016. The connection types used to access the internet at home are 86.8% of fixed broadband connections (fixed broadband connections), followed by mobile broadband connections (43.2%) and Narrowband connections (10.3%). Considering the fact that in 2003, only 22% of the population owned a PC, and barely 7% were connected to the Internet, we have a picture of the leap that Internet had in Romania. The Internet, whether accessed via fixed or mobile devices, offers more and richer affordances than earlier generations of communications technologies [2]. The downside consists in the increasing number of threats and attacks that are threatening the proper functioning of the Internet.

The internet spread produced major transformations in the Romanian society. The new connectivity transformed people into global citizens, making them aware of the digital rights and benefits. The internet was the platform for creating new products and services, for developing the economy or for enhancing the business to business, government to business, government to citizen processes.

5 Internet Domains in Romania - activities and challenges

As the discussion is evolving towards a global cyberspace, a major part of world population uses the Internet – roughly 40% of global population, we can observe this is a double-sided sword to governance: on one side, we see the characteristics of promoting cyberspace tenure, governance, and providing convenient conditions to function, and on the other side it raises unprecedented challenges and threats, some internals, others represented by the eroding of geographic borders of the states [8].

Even though the empirical evidence at an aggregate level is inconsistent, the positive effects of computers and information technology on productivity nowadays are taken for granted. Internet connectivity is seen as instrumental for a range of policy objectives, including the creation of high-quality jobs, improvements in the quality of life, and the safeguarding of environmental goals [2].

Despite the stunning advances in the technology sector in recent decades the location will retain its importance. In this context the national domain names are of high importance.

The Romanian Top Level Domain performs a vital role in the information society. Its reliability and security are essential for the social and economic activities and for the proper functioning of the on-line services.

Often times the Domain Name System is seen as just a technical task, but the administration involves a lot more facts, such as infrastructure stability, system security and resource allocation. DNS is not just a function in the Internet governance as DNS englobes technologies that contribute to the Internet functioning. The DNS embeds content; the domains names contain text (letters and/or numbers) and therefore involve conflicts in matter of property. The system must have

several points in which the access to the content is sanitized and verified.
When it comes to Internet governance, security has a key role, and this topic constitutes a major concern at country and ccTLD level and also for the governing bodies of Internet, as there are ICANN and IANA [6]. The organizations that ensure the Internet governance are always updating their security policies and organize training and advisory sessions on different levels in order to countermeasure the security threats. For every ccTLD, security is a continuous topic as the security risks are not something that can be tolerated at this level.

The principles that govern the activity of RoTLD are:

1. equal treatment of all requests in the order they are received on a "first-come, first served";
2. ensure high availability for *.ro* domain registration services;
3. ensure security of access to nameservers;
4. backup DNS database, WHOIS, for all areas managed in the .ro;
5. facilities for finding domain availability, through standard query service on the server whois.rotld.ro or using www.rotld.ro;
6. maximum efficiency in the available time working and technical conditions;
7. ensure the protection of trademarks and names of public figures, therefore is not allowed registration of a domain name in order to be resold.

The proper management of DNS raises a wide palette of issues that must be considered and handled accordingly. The Internet engineers designed the DNS in 1984, before the network internationalization and in an environment characterized by trust among its users [5]. With the Internet expansion, the security of the DNS has been a challenge for all the engineers in order to protect the systems against the increasing number and types of attacks.

Security means the integrity, reliability, and confidentiality of the system. At the dawn of the internet, organizations have not assigned a significant role to security, relying primarily on mitigating the damages caused by attacks rather than preventing them. Public awareness of security breaches increased dramatically when high profile Internet companies like Amazon, eBay, and Yahoo were hit by denial-of-service (DDoS) attacks in February 2000 [10].

The cyber criminals are nowadays becoming more sophisticated and are investing major amounts in research and development and infrastructure and are even organized in international networks [4]. Frequent attacks on the DNS have to do with the domain lookup process and are attempting to redirect visitors to fake sites with the sole purpose of censorship, fraud, or identity theft. The DDoS attacks are very disruptive for the Internet functioning as these attacks are sending traffic to the servers from multiple sources until the servers are jammed and unable to respond.

The electronic system at RoTLD is composed by several apps. The automatic system of .ro domain registration was built before 2008, and it implemented an automatic registration procedure for the .ro Registrars. The procedure is based on the EPP protocol for communication between RoTLD and its partners.

Besides the interfaces that are provided to the Registrars, RoTLD is made up of many other dedicated applications for the management of .ro domains: *WHOIS service, internal applications used by operators, billing applications, log records*; all these applications are implemented independently using different architectures, different databases having different requirements. Administrative cost was higher as some applications conflicted if they were installed on the same server. Given this situation, the development of a middleware component was imposed.

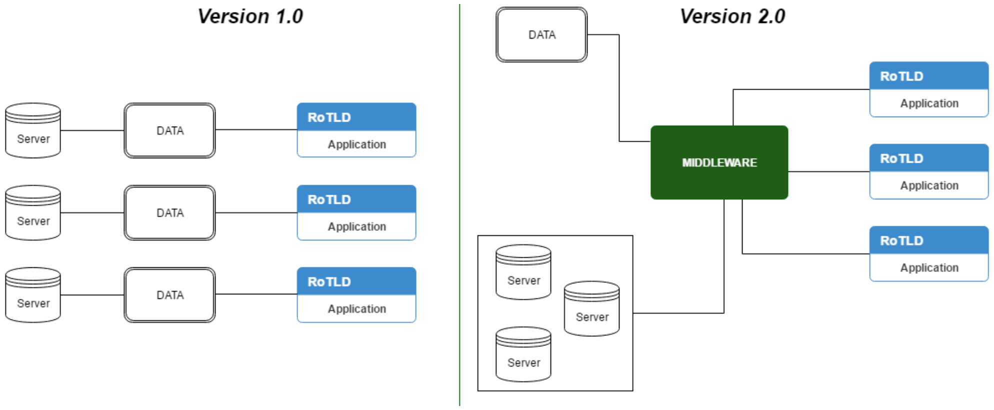

Figure 1 - The transition from the original system to the Middleware-based system

The middleware implement the necessary methods for application communication: working with databases, ”logs” or diary records, distributed computing, statistics.

The middleware ensures [7]:

1. remote access to the implemented methods, via an interface using established, standardized protocols and which do impose bans at the level of the programming language;

2. authorization access based on credentials, digital signatures and network-level restrictions;

3. automatic distribution of requests from the access interface towards the available resources;

4. the recording of each request and its state in a journal, as well as the availability of request analysis.

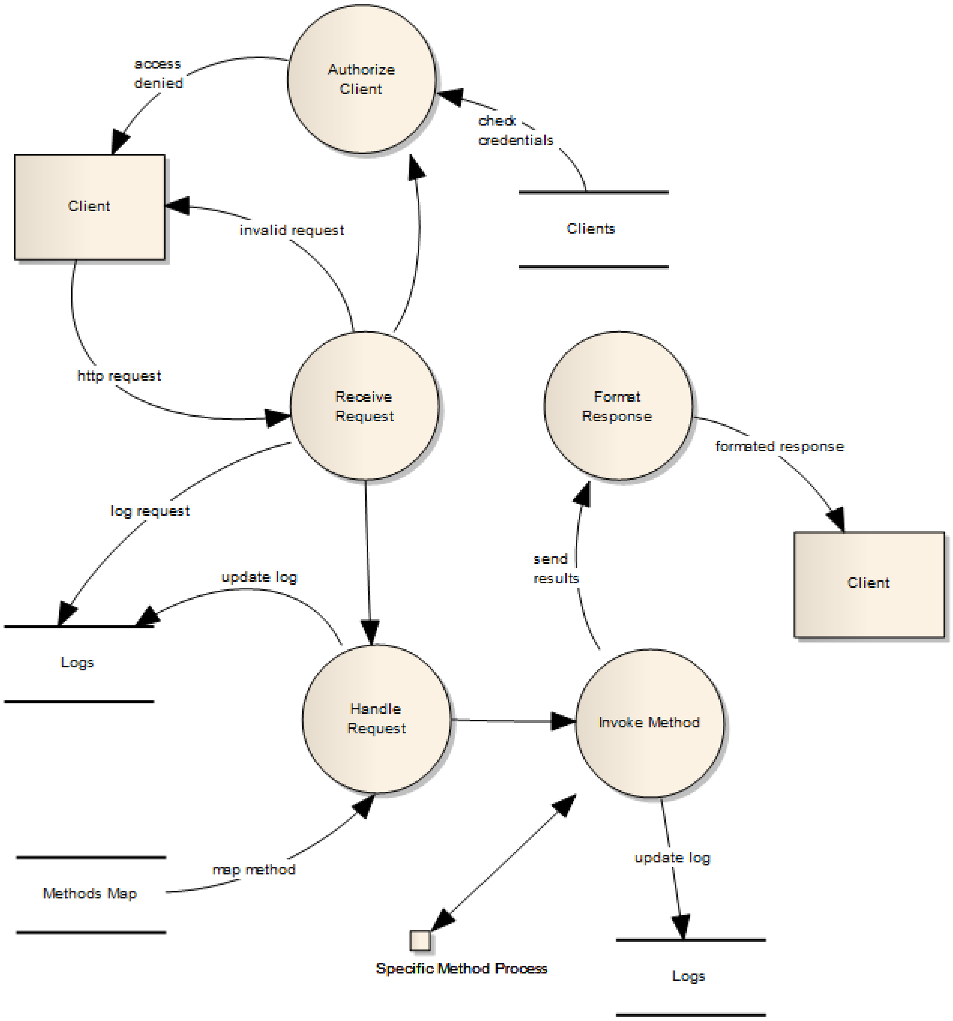

Figure 2 - Information paths and routes in the Middleware

Security challenges in the management of .ro domains

The **security concepts** in the area of internet domain names is based on the fact that the applications accessible via HTTP protocol have the following characteristics [7]:

1. CAPTCHA code, which is unique on each HTTP request;
2. TOKEN, also unique on each HTTP request that prevents *Cross Site Request Forgery*;
3. Data cleaning on the incoming HTML and Javascript elements, to prevent *Cross Site Scripting*;
4. Validation and sanitization of web forms accordingly with the internal procedures, to prevent *Cross Site Scripting* and *SQL injection;*

5. Secured cookies attributes;

6. Efficient sessions management (which are stored in RAM memory to provide faster access to session data) by using a separate service;

7. Complete cookie opacity to prevent disclosure of the data associated to the cookie;

8. Count access to certain resources with eventual temporary restriction, to prevent the *Brute Force* attack on that resource;

9. Set up the WWW service to automatically identify and block certain (malicious) ways for sending HTTP requests and malicious URLs;

10. WWW service configuration so as not to disclose information about the software modules or the operating system;

11. WWW service is configured with a 2048-bit digital certificate that provides a high level of security of HTTP requests;

12. the WWW service is protected and receives an SSL accelerator Reversed Proxy configuration which, in addition, adjusts certain parameters of TCP / IP communications between end-points;

13. Firewall for the WWW service to ensure packet sanitization and reassembly based on TCP/IP; classification of traffic by type of services; pro-active protection to *Brute-Force* attacks.

The DNSSEC (DNS Security Extensions) was adopted by RoTLD to provide a layer of authentication when it comes to domain lookup. Unfortunately the DNSSEC involves work also from the Registrars in setting the servers so the DNSSEC adoption is at a very slow rate.

The security of DNS is not an issue for average users, but people must be aware of the threats. For example people should consider the difference between HTTP and HTTPS connection on the e-commerce sites.

6 Conclusions

The information society englobes a wide range of terms and activities. The central core that ensures its existence is the Internet and subsequently the Domain Name System that maintains its proper functioning. The major scope of the web domains is to contribute to a real global Information Society for each citizen, where any member can access, use, create and share information, therefore unleash the utmost potential in the individuals.

While for the vast majority of the population it does not represent a concern, the DNS governance and functioning raises a lot of policy issues and technical challenges.

Even though protocols and procedures exist to mitigate the cyber-attacks, the DNS is still vulnerable to threats as the adoption rate of security solutions is less than the rate of the attacks to the DNS.

Besides the technical engineering that is involved in the system, there is also about the policy that governs the DNS. The policymakers in this domain must understand the very complex processes that maintain the proper functioning of the Internet, and must establish the laws accordingly, but without imposing rules that might censor the users' right to digital information and speech.

RoTLD has increased the security policies and this led to a lowering of the vulnerabilities in the entire system. DNSSEC was implemented and all the beneficiaries of the domains system are encouraged to make use of it. Also the registrars are advised to strengthen their procedures for domain registration and administration. RoTLD is keen on maintaining its value, which was achieved over the years, and is always focused on preserving a high security. The programs that are used are periodically tested against security breaches and investments are made in network equipment.

References

[1] Banciu, D., Boncea, R.M., Rotuna, C.I., Anghel, M., *Bringing EU Entrepreneurs together through Cross-border Services SPOCS – a Case Study*, Studies in Informatics and Control (2012).

[2] Bauer, J.M., *Inequality in the Information Society*, SSRN Electronic Journal (2016).

[3] Bradshaw, S., DeNardis, L., *The politicization of the Internet's Domain Name System: Implications for Internet security, universality, and freedom*, New Media & Society (2016).

[4] Mohan, R., *Cyber Security Outlook for TLD operators,* APTLD Meeting in Manila (2009).

[5] Plante, N.A., *Practical Domain Name System Security: A survey of Common Hazards and Preventative Measures* (2004).

[6] Rajasekera, J., Das, S., *Do the Internet Security Alerts Have an Impact on Lowering ccTLD Security Risks* (2010).

[7] Sandu, I.E., Peta B., Leanca C., Dumitrache M., Boncea R., Staicut E., *Internet si domeniile .ro* (2011).

[8] Shen, Y., *Cyber Sovereignty and the Governance of Global Cyberspace*, Springer (2016).

[9] Soldi, R., et al, *Towards a new update of the Digital Agenda and creation of the Digital Single Market: challenges and opportunities for Local and Regional Authorities in the European Union* (2015).

[10] Staicut, E., Boncea, R., Rotuna, C.I., *A Reliable Architecture for a Massive and Continuous Scanner of Web Vulnerabilities in Internet* (2016).

[11] Toffler, A., *The third wave* (1981).

[12] https://www.icann.org/resources/pages/what-2012-02-25-en, accessed in April 2017