An Overview of the Status of DNS and HTTP Security Services in Higher Education Institutions in Portugal

Nuno Felgueiras[1] and Pedro Pinto[1,2](✉)

[1] Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal
nunofelgueiras@ipvc.pt
[2] ISMAI, 4475-690 Maia, and INESC TEC, 4200-465 Porto, Portugal
pedropinto@estg.ipvc.pt

Abstract. Currently, there are several security-related standards and recommendations concerning Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP) services, that are highly valuable for governments and their services, and other public or private organizations. This is also the case of Higher Education Institutions (HEIs). However, since these institutions have administrative autonomy, they present different statuses and paces in the adoption of these web-related security services.

This paper presents an overview regarding the implementation of security standards and recommendations by the Portuguese HEIs. In order to collect these results, a set of scripts were developed and executed. Data were collected concerning the security of the DNS and HTTP protocols, namely, the support of Domain Name System Security Extensions (DNSSEC), HTTP main configurations and redirection, digital certificates, key size, algorithms and Secure Socket Layer (SSL)/Transport Layer Security (TLS) versions used.

The results obtained allow to conclude that there are different progresses between HEIs. In particular, only 11.7% of HEIs support DNSSEC, 14.4% do not use any SSL certificates, 74.8% use a 2048 bits encryption key, and 81.1% use the Rivest-Shamir-Adleman (RSA) algorithm. Also, 6.3% of HEIs still negotiate with the vulnerable SSLv3 version.

Keywords: DNSSEC · HTTP · Higher education · Academic · Institutions · SSL · Security

1 Introduction

Currently, there are several security-related standards and recommendations concerning Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP) services. A subset of these standards and recommendations intend to secure the DNS service, i.e. the Domain Name System Security Extensions (DNSSEC) [16–18], and others intended to secure HTTP service. The later, includes Hyper Text Transfer Protocol Secure (HTTPS) [15], Secure Socket

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 457–469, 2022.
https://doi.org/10.1007/978-3-031-06371-8_30

Layer (SSL) certificates and SSL/Transport Layer Security (TLS) protocols [7,12,23].

The implementation of these current security standards and recommendations is highly valuable and strongly encouraged for governments and their services, and other public or private organizations [9]. Recent efforts such as the ones described in [5,19,22] had been carried out to analyse, check, evaluate, and report the evolution and adoption of these services in multiple countries, domains and institution.

Educational institutions should also follow these security standards and recommendations. However, since in Portugal [11] and in Europe [2], the Higher Education Institutions (HEIs) have administrative autonomy, this implies different statuses and paces in the adoption of these web-related security services, both in the public and private institutions.

This paper provides an overview of the security status regarding the adoption of DNS and HTTP security services on the Portuguese HEIs. A set of scripts were developed to collect and analyze each of these main protocols (DNS and HTTP) security implementations. Specific data was collected and analyzed regarding the adoption of DNSSEC, the HTTP redirection, and the information regarding SSL certificates (in particular the Certificate Authority (CA), Key Size and Signature types used).

The remainder of this document is organized as follows: Sect. 2 presents the related work. Section 3 introduces the methodology used to obtain the results; Sect. 4 presents the results; Lastly, Sect. 5 presents the conclusions.

2 Related Work

Given that DNS protocol does not implement security mechanisms in its initial versions, there are a set of standards intended to enhance the security of this protocol. The secure version of DNS, including DNSSEC, have been available since 2005 in [16–18]. By mirroring the DNS hierarchy, DNSSEC authenticates the DNS responses and prevents modified or forged DNS records.

A set of efforts have been made to implement DNS Security. Authors in [21] present an analysis regarding the misconfigurations for DNS domains and state that, although progress has been made in the implementation of DNSSEC, over 4% of evaluated domains show misconfigurations. In [10] the authors study the security of DNSSEC deployment at scale, particularly in Top Level Domains (TLDs) that offer economic incentives. They find that DNSSEC implementations in the wild poorly reflects standard recommendations, and, on average, large operators deploy weak DNSSEC security more frequently than small operators. In [19] the authors present a research of the evolution and adoption of top Level Domains and DNSSEC in New Zealand. The study highlights that, the rapid increase in the number of gTLDs give registrants a wider choice of domain names, but it also offers malicious actors more opportunities to attack. It is concluded that DNSSEC deployment at New Zealand national level to be improving but still weaker than global averages. Efforts need to be made to ensure correct

Delegation Signed records are uploaded to the registry to complete the DNSSEC chain of trust.

Standards have been proposed to provide HTTP Security. The SSLv1 was never publicly released. In 1995, SSLv2 [7] has been released but, since its release, it presented security weaknesses and has been replaced in 1996 by the SSLv3 [8]. In 1999, the TLSv1.0 [4] was released and was based on the deprecated SSL Protocol, which was followed in 2006 by the TLSv1.1 [6], in 2008 by TLSv1.2 [14] and, in 2018, the latest was released, the TLSv1.3 [13].

A set of research works are focused on the progress of the implementation of HTTP security. In [22] the authors survey the usage of RC4 stream cipher in online web portals of Sri Lankan Banking and Non-Banking Financial Sector, as well as the awareness level of the Network Security Administrating staff of some of the selected banks which are geographically based in Sri Lanka, regarding the usage of RC4 in SSL. This study revealed that 75% of the Banking and Non-Banking Financial Institutes in Sri Lanka have been upgraded to TLS1.2 from SSL and TLS older versions and hence they have mitigated the RC4 vulnerabilities. In [5], there were measures taken to prevent eavesdropping and tampering a set of Internet protocols that rely on TLS, the authors quantify the adoption of TLS using passive traffic traces captured on a backbone and edge academic network in Japan, monitoring the evolution of five common protocols and their TLS-variants over ten years of traffic data. They found that the adoption of TLS for HTTP only started being significantly used around 2012, while IMAP traffic is mostly encrypted for the last ten years. The deployment of HTTPS is mainly driven by large content providers and migrating the remaining HTTP traffic to HTTPS might require significant efforts as it concerns numerous smaller services who may face compatibility concerns. In [20] the research author, provided a status survey of SSL/TLS sites in 2018 after "search form" issues have been raised. From 2014, several researchers conducted monitored SSL/TLS sites using the top level domain ".jp" based on a URL list extracted from Alexa Top Sites [3], and investigated the usage rate of SSL/TLS versions and Export-grade encryption algorithms. They also pointed out that online login sites belonging to associations of Japanese banks were well-controlled in SSL/TLS server configurations and content management, however ordinary sites had "search form" issues.

3 Methodology

In the initial step of this analysis, a list of all HEIs was collected from the information on the Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) website in [1] and resulted in a list with a total of 320 results. Using two scripts, the 320 were collected and filtered to obtain only the main office or university center. The first script was intended to collect all the links to access detailed information for each HEI and, the second, to access the links previously collected to obtain the information. The scripts were made in PHP using the *file_get_contents* function in order to obtain the HTTP code of the pages and the data obtained by them filtered with *regex*. After filtering the data, a total of 111 HEIs were obtained distributed across the 18 districts and 2 autonomous regions of Portugal. For the collected HEIs, the following set of items were analysed in their implementation or configuration:

- DNS
  - DNSSEC
- HTTP
  - Configuration and Redirection
  - SSL Certificate
    - Certificate Authority
    - Key Size
    - Algorithm
  - SSL/TLS Versions
    - SSLv2, v3
    - TLSv1.0, v1.1, v1.2, v1.3

Three scripts were developed with the following functions:

- Script 1 - Collect the state of DNSSEC
  To capture the state of DNSSEC, the *php-dnssec-validator* library was used in order to know if the institution's domain had DNSSEC and if so, the script would save the Key, KeyTag and Algorithm Values in the database.
- Script 2 - Collect SSL Certificates Information
  To collect information from SSL certificates, the *stream_socket_client* function was used along with openssl in order to obtain information such as CA, Key size and Signature Types.
- Script 3 - Test the negotiation of SSL/TLS protocols
  To test the SSL/TLS negotiations, the script's job was to try to establish a communication for each of the protocols, that is, SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 and the most recent TLSv1.3. To accomplish this, we used the PHP function *stream_socket_client*, with the exception of TLSv1.3 which required the use of *curl* due to compatibility issues.

With the Location data, two more types of information were obtained. Using *regex* it was possible to know if the forwarding was to the same domain or not and if it was already forwarded to a secure connection (HTTPS). The process of developing the scripts and executing them to collect data and was carried out in full during the month of April 2021.

4 Results and Analysis

Table 1 it is possible to see the distribution of HEIs by districts of Portugal, as well as by environment of institution (public or private). The Fig. 1 draws the results of the Table 1.

The district of Lisboa has the highest number of HEIs, followed by Porto and Coimbra. The districts of Beja, Bragança, Évora, Guarda, Ponta Delgada and Viseu only have one HEI, and the district of Porto has a higher count of private

Table 1. Districts with public and private institutions

District	Global		Public		Private	
	#	%	#	%	#	%
Aveiro	5	4,5%	1	20,0%	4	80,0%
Beja	1	0,9%	1	100,0%	0	0,0%
Braga	4	3,6%	2	50,0%	2	50,0%
Bragança	1	0,9%	1	100,0%	0	0,0%
Castelo Branco	2	1,8%	2	100,0%	0	0,0%
Coimbra	10	9,0%	8	80,0%	2	20,0%
Évora	1	0,9%	1	100,0%	0	0,0%
Faro	2	1,8%	1	50,0%	1	50,0%
Funchal	3	2,7%	1	33,3%	2	66,7%
Guarda	1	0,9%	1	100,0%	0	0,0%
Leiria	3	2,7%	1	33,3%	2	66,7%
Lisboa	35	31,5%	15	42,9%	20	57,1%
Ponta Delgada	1	0,9%	1	100,0%	0	0,0%
Portalegre	5	4,5%	5	100,0%	0	0,0%
Porto	25	22,5%	4	16,0%	21	84,0%
Santarém	4	3,6%	3	75,0%	1	25,0%
Setúbal	3	2,7%	2	66,7%	1	33,3%
Viana do Castelo	2	1,8%	1	50,0%	1	50,0%
Vila Real	2	1,8%	1	50,0%	1	50,0%
Viseu	1	0,9%	1	100,0%	0	0,0%
Total:	**111**	**100%**	**53**	**47,7%**	**58**	**52,3%**

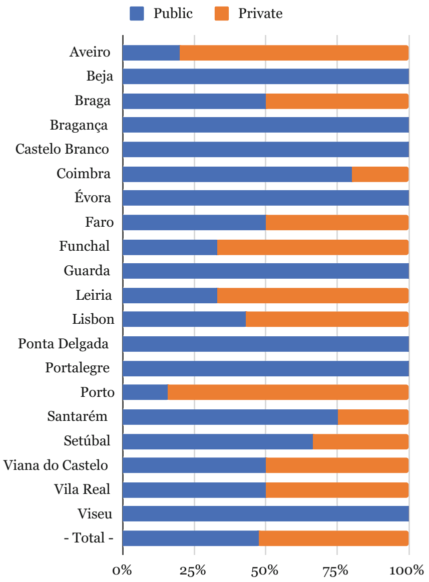

Fig. 1. Districts public/private

institutions. The districts of Beja, Bragança, Castelo Branco, Évora, Guarda, Ponta Delgada, Portalegre and Viseu only have public institutions.

Table 2 presents the results regarding the implementation of DNSSEC on public and private HEIs. Figure 2 draws the results of the Table 2. From these results it can be verified that more than 80% of HEIs do not implement DNSSEC. Less than 75% of HEIs in the districts of Coimbra and Lisboa have DNSSEC implemented. In the districts of Braga, Faro, Santarém and Vila Real only 50% of HEIs have implemented DNSSEC. In the district of Évora the only exising HEIs implements DNSSEC. In the district of Lisboa there is only one private institution that implemented DNSSEC, representing only 0.9% from the total. On public institutions, 10.8% implemented DNSSEC.

Table 3 presents the status on HTTP and HTTPS, namely described using the following conditions:

- HTTP Only: Websites with only HTTP protocol enabled, who do not provide any sort of security
- HTTP & HTTPS: Websites that have both HTTP and HTTPS active. They can be accessed by both protocols, given that they do not have any type of redirects to force HTTPS to be used;
- Invalid SSL Config: Websites that have implemented HTTPS/SSL but misconfigured it. These are websites that may be reachable and look like they are functional, but upon analysis, we found that the certificate information is

Table 2. DNSSEC public/private per districts

District	Total	Without DNSSEC		DNSSEC public		DNSSEC private	
	#	#	%	#	%	#	%
Évora	1	0	0,0%	1	100,0%	0	0,0%
Braga	4	2	50,0%	2	50,0%	0	0,0%
Faro	2	1	50,0%	1	50,0%	0	0,0%
Santarém	4	2	50,0%	2	50,0%	0	0,0%
Vila Real	2	1	50,0%	1	50,0%	0	0,0%
Coimbra	10	8	80,0%	2	20,0%	0	0,0%
Lisboa	35	31	88,6%	3	8,6%	1	2,9%
Aveiro	5	5	100,0%	0	0,0%	0	0,0%
Beja	1	1	100,0%	0	0,0%	0	0,0%
Bragança	1	1	100,0%	0	0,0%	0	0,0%
Castelo Branco	2	2	100,0%	0	0,0%	0	0,0%
Funchal	3	3	100,0%	0	0,0%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%
Leiria	3	3	100,0%	0	0,0%	0	0,0%
Ponta Delgada	1	1	100,0%	0	0,0%	0	0,0%
Portalegre	5	5	100,0%	0	0,0%	0	0,0%
Porto	25	25	100,0%	0	0,0%	0	0,0%
Setúbal	3	3	100,0%	0	0,0%	0	0,0%
Viana do Castelo	2	2	100,0%	0	0,0%	0	0,0%
Viseu	1	1	100,0%	0	0,0%	0	0,0%
Total:	**111**	**98**	**88,3%**	**12**	**10,8%**	**1**	**0,9%**

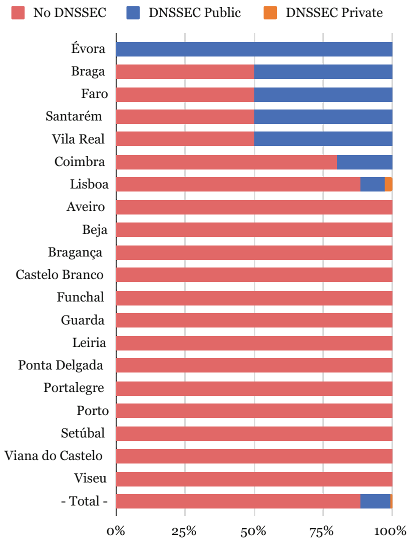

Fig. 2. Differences public/private institutions using DNSSEC

incomplete due to lack of an Intermediate Chain. Example: If a visitor who has never accessed a particular website which its certificate was issued by "Let's Encrypt", and that particular site does not have an intermediate chain, the browser will say that the website has an invalid certificate because it can not verify whether or not the intermediate certificate is valid; However, if that visitor has previously visited another website that had its certificate issued by "Let's Encrypt" as well and, in this case, the website has a valid intermediate certificate, the browser will remember and trust that chain, which results in that particular chain (Let's Encrypt) not being checked by the browser again;

- HTTP to HTTPS (Other): Websites that forward the visitor to a secure page outside of the main domain.
- HTTP to HTTPS (Same): Websites that forward the visitor to a secure page within the main domain.

Figure 3 draws the results of the Table 3. From the results obtained it can be verified that the districts of Beja, Évora, Faro, Ponta Delgada, Viana do Castelo, Vila Real and Viseu HEIs redirect visitors to HTTPS in the same domain. Districts of Lisboa, Porto and Santarém HEIs also redirect the visitors to HTTPS but using others domains. Also, the districts of Lisboa, Coimbra and Porto HEIs also have websites with invalid SSL configuration (without chain). Regarding the districts of Aveiro, Funchal, Lisboa, Coimbra, Porto, Castelo Branco,

Table 3. Web security in the academic institutions per district

Districts	Total	HTTP only		HTTP & HTTPS		Invalid SSL config		HTTP to HTTPS (other)		HTTP to HTTPS (same)	
	#	#	%	#	%	#	%	#	%	#	%
Beja	1	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Évora	1	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Faro	2	0	0,0%	0	0,0%	0	0,0%	0	0,0%	2	100,0%
Ponta Delgada	1	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Viana do Castelo	2	0	0,0%	0	0,0%	0	0,0%	0	0,0%	2	100,0%
Vila Real	2	0	0,0%	0	0,0%	0	0,0%	0	0,0%	2	100,0%
Viseu	1	0	0,0%	0	0,0%	0	0,0%	0	0,0%	1	100,0%
Aveiro	5	0	0,0%	1	20,0%	0	0,0%	0	0,0%	4	80,0%
Funchal	3	0	0,0%	1	33,3%	0	0,0%	0	0,0%	2	66,7%
Leiria	3	1	33,3%	0	0,0%	0	0,0%	0	0,0%	2	66,7%
Lisboa	35	7	20,0%	3	8,6%	1	2,9%	3	8,6%	21	60,0%
Coimbra	10	2	20,0%	1	10,0%	1	10,0%	0	0,0%	6	60,0%
Porto	25	3	12,0%	5	20,0%	2	8,0%	1	4,0%	14	56,0%
Castelo Branco	2	0	0,0%	1	50,0%	0	0,0%	0	0,0%	1	50,0%
Santarém	4	1	25,0%	0	0,0%	0	0,0%	1	25,0%	2	50,0%
Braga	4	1	25,0%	1	25,0%	0	0,0%	0	0,0%	2	50,0%
Setúbal	3	0	0,0%	2	66,7%	0	0,0%	0	0,0%	1	33,3%
Bragança	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%	0	0,0%
Portalegre	5	0	0,0%	5	100,0%	0	0,0%	0	0,0%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%
Total:	**111**	**16**	**14,4%**	**21**	**18,9%**	**4**	**3,6%**	**5**	**4,5%**	**65**	**58,6%**

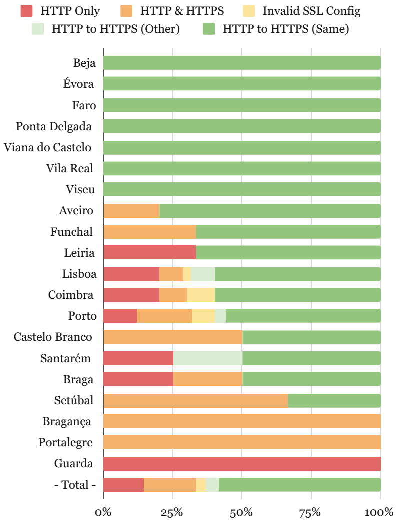

Fig. 3. HTTPS per district

Braga, Setúbal, Bragança and Portalegre, their HEIs have websites with SSL certificates but do not force their usage. The districts of Leiria, Lisboa, Coimbra, Porto, Samtarém, Braga and Guarda have websites without any SSL certificates.

Table 4 presents the CAs used by all the HEIs on public and private HEIs. Figure 4 draws the results of the Table 4. From the results obtained regarding public institutions, 41.5% use *GEANT* and 18.9% use *TERENA*. 13.2% of these institutions use free certificates provided by *Let's Encrypt*, and 15.1% do not use any SSL certificates at all. Regarding the private institutions, 22.4% use free certificates provided by *Let's Encrypt*, 17.2% use *GEANT*, and 8.6% use *Sectigo* as their CA; 20.7% do not use any SSL certificate at all.

Table 4. CAs used by HEIs

CA	Global		Public		Private	
	#	%	#	%	#	%
GEANT Vereniging	32	28,8%	22	19,8%	10	9,0%
No Certificate	20	18,0%	8	7,2%	12	10,8%
Let's Encrypt/R3	20	18,0%	7	6,3%	13	11,7%
TERENA	14	12,6%	10	9,0%	4	3,6%
Sectigo Limited	9	8,1%	4	3,6%	5	4,5%
GlobalSign nv-sa	5	4,5%	0	0,0%	5	4,5%
DigiCert Inc	3	2,7%	0	0,0%	3	2,7%
Cloudflare, Inc.	2	1,8%	1	0,9%	1	0,9%
cPanel, Inc.	2	1,8%	0	0,0%	2	1,8%
GoDaddy.com, Inc.	2	1,8%	0	0,0%	2	1,8%
GoGetSSL	1	0,9%	0	0,0%	1	0,9%
MULTICERT	1	0,9%	1	0,9%	0	0,0%
Total:	**111**	**100,0%**	**53**	**47,7%**	**58**	**52,3%**

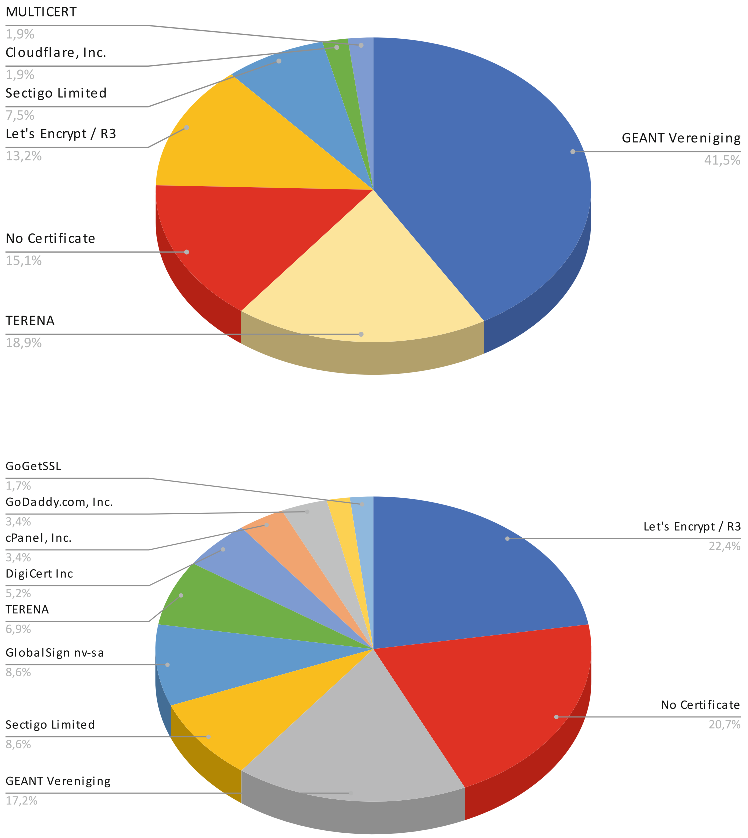

Fig. 4. CAs of public HEIs (above), and private HEIs (below)

Table 5 presents the size of the SSL keys used by the HEIs. Figure 5 draws the results of the Table 5. In regards to the key lenght of Rivest-Shamir-Adleman (RSA) keys used, 50% of HEI websites of the district of Castelo Branco district use 4096 bits RSA keys, 25% of websites on the district of Braga use 4096 bits RSA keys, only one HEIs in the district of Porto uses a 256 bits Elliptic Curve Cryptography (ECC) key. HEIs in the districts of Beja, Évora, Ponta Delgada, Viana do Castelo, Vila Real, Aveiro, Faro, Funchal, Viseu, Setúbal, Bragança and Portalegre use 2048 bits RSA keys.

Table 5. SSL key lenght by district

Districts	Total	Without SSL		2048 (RSA)		4096 (RSA)		256 (ECC)	
		#	%	#	%	#	%	#	%
Castelo Branco	2	0	0,0%	1	50,0%	1	50,0%	0	0,0%
Braga	4	1	25,0%	2	50,0%	1	25,0%	0	0,0%
Porto	25	5	20,0%	16	64,0%	3	12,0%	1	4,0%
Coimbra	10	3	30,0%	6	60,0%	1	10,0%	0	0,0%
Lisboa	35	8	22,9%	26	74,3%	1	2,9%	0	0,0%
Beja	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Évora	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Ponta Delgada	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Viana do Castelo	2	0	0,0%	2	100,0%	0	0,0%	0	0,0%
Vila Real	2	0	0,0%	2	100,0%	0	0,0%	0	0,0%
Aveiro	5	0	0,0%	5	100,0%	0	0,0%	0	0,0%
Faro	2	0	0,0%	2	100,0%	0	0,0%	0	0,0%
Funchal	3	0	0,0%	3	100,0%	0	0,0%	0	0,0%
Viseu	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Setúbal	3	0	0,0%	3	100,0%	0	0,0%	0	0,0%
Bragança	1	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Portalegre	5	0	0,0%	5	100,0%	0	0,0%	0	0,0%
Santarém	4	1	25,0%	3	75,0%	0	0,0%	0	0,0%
Leiria	3	1	33,3%	2	66,7%	0	0,0%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%	0	0,0%
Total	**111**	**20**	**18,0%**	**83**	**74,8%**	**7**	**6,3%**	**1**	**0,9%**

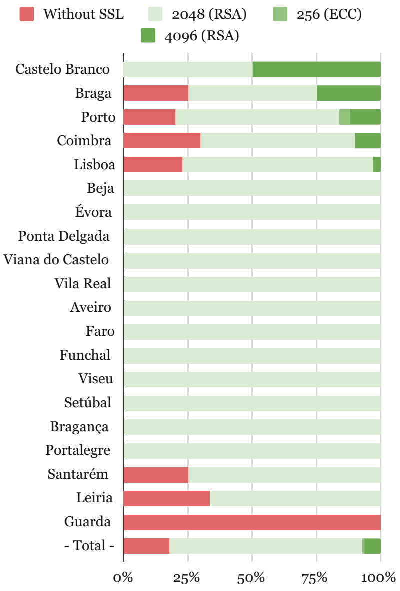

Fig. 5. SSL Key lenght

Table 6 presents the algorithms used by the HEIs per district. Figure 6 draws the results of the Table 6. From the results obtained it can be verified that only one HEI in the district of Porto uses the ECC algorithm, 13 districts use the algorithm RSA, and in the districts of Lisboa, Porto, Braga, Santarém, Coimbra, Leiria and Guarda, the HEIs do not use any algorithm.

Table 7 presents the results on the SSL/TLS versions used by HEIs in their websites. These results are presented in a decreasing order from top (better) to bottom (worst). Figure 7 draws the results of the Table 7. The results show that more than 25% of HEIs in the districts of Porto, Lisboa, Leiria, Funchal and Setúbal already negotiate on the most recent TLSv1.3 version. 25% of HEIs in Santarém negotiate on TLSv1.1 version and, in the remaining HEIs, the best negotiation method is accomplished with the TLSv1.2 version. No data is presented regarding SSLv3 and TLS1.0 since better versions are supported by the HEIs. No data is presented regarding SSLv2 since none of the websites have negotiated with this protocol.

Table 8 presents the results for the worse options offered by the HEIs regarding the negotiation mechanisms. These results are presented in a decreasing order from top (better) to bottom (worst). Figure 8 draws the results of the Table 8. In regards to the TLS ciphers used by the HEIs analyzed, more than 25% of the districts of Portalegre, Viana do Castelo, Castelo Branco, Lisboa, Aveiro, Porto and Setúbal HEIs do not negotiate under TLSv1.2. The districts of Setúbal, Coimbra and Leiria also have HEIs that do not negotiate below TLSv1.1. All HEIs from the districts of Beja, Évora, Ponta Delgada, Vila Real, Faro and Viseu

Table 6. SSL Algorithms by district

Districts	Total	Without SSL		RSA		ECC	
	#	#	%	#	%	#	%
Castelo Branco	2	0	0,0%	2	100,0%	0	0,0%
Beja	1	0	0,0%	1	100,0%	0	0,0%
Évora	1	0	0,0%	1	100,0%	0	0,0%
Ponta Delgada	1	0	0,0%	1	100,0%	0	0,0%
Viana do Castelo	2	0	0,0%	2	100,0%	0	0,0%
Vila Real	2	0	0,0%	2	100,0%	0	0,0%
Aveiro	5	0	0,0%	5	100,0%	0	0,0%
Faro	2	0	0,0%	2	100,0%	0	0,0%
Funchal	3	0	0,0%	3	100,0%	0	0,0%
Viseu	1	0	0,0%	1	100,0%	0	0,0%
Setúbal	3	0	0,0%	3	100,0%	0	0,0%
Bragança	1	0	0,0%	1	100,0%	0	0,0%
Portalegre	5	0	0,0%	5	100,0%	0	0,0%
Lisboa	35	8	22,9%	27	77,1%	0	0,0%
Porto	25	5	20,0%	19	76,0%	1	4,0%
Braga	4	1	25,0%	3	75,0%	0	0,0%
Santarém	4	1	25,0%	3	75,0%	0	0,0%
Coimbra	10	3	30,0%	7	70,0%	0	0,0%
Leiria	3	1	33,3%	2	66,7%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%
Total	**111**	**20**	**18,0%**	**90**	**81,1%**	**1**	**0,9%**

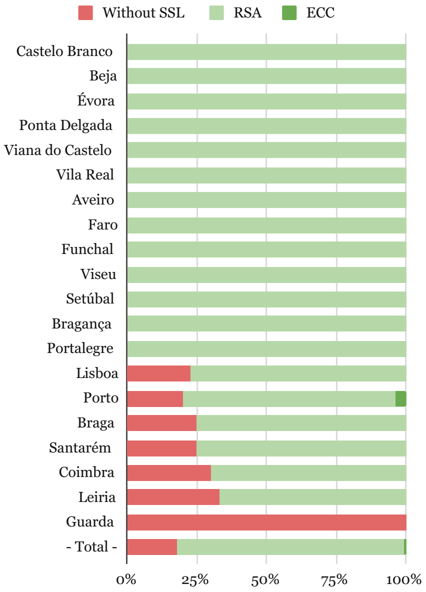

Fig. 6. SSL algorithms

Table 7. Best supported SSL/TLS versions

Districts	Total	Without TLS/SSL		TLSv1.1		TLSv1.2		TLSv1.3	
	#	#	%	#	%	#	%	#	%
Porto	25	2	8,0%	0	0,0%	14	56,0%	9	36,0%
Lisboa	35	5	14,3%	0	0,0%	18	51,4%	12	34,3%
Leiria	3	1	33,3%	0	0,0%	1	33,3%	1	33,3%
Funchal	3	1	33,3%	0	0,0%	1	33,3%	1	33,3%
Setúbal	3	1	33,3%	0	0,0%	1	33,3%	1	33,3%
Santarém	4	0	0,0%	1	25,0%	2	50,0%	1	25,0%
Aveiro	5	0	0,0%	0	0,0%	4	80,0%	1	20,0%
Coimbra	10	2	20,0%	0	0,0%	7	70,0%	1	10,0%
Beja	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Évora	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Ponta Delgada	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Viana do Castelo	2	0	0,0%	0	0,0%	2	100,0%	0	0,0%
Vila Real	2	0	0,0%	0	0,0%	2	100,0%	0	0,0%
Faro	2	0	0,0%	0	0,0%	2	100,0%	0	0,0%
Viseu	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Bragança	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%
Portalegre	5	0	0,0%	0	0,0%	5	100,0%	0	0,0%
Braga	4	1	25,0%	0	0,0%	3	75,0%	0	0,0%
Castelo Branco	2	1	50,0%	0	0,0%	1	50,0%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%	0	0,0%
Total:	**111**	**15**	**13,5%**	**1**	**0,9%**	**68**	**61,3%**	**27**	**24,3%**

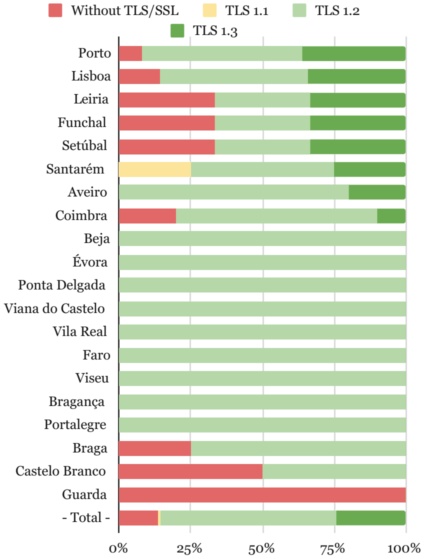

Fig. 7. Best supported SSL/TLS Versions

Table 8. Worst supported SSL/TLS versions

Districts	Total	Without TLS/SSL		SSLv3		TLSv1.0		TLSv1.1		TLSv1.2	
	#	#	%	#	%	#	%	#	%	#	%
Portalegre	5	0	0,0%	0	0,0%	1	20,0%	0	0,0%	4	80,0%
Viana do Castelo	2	0	0,0%	0	0,0%	1	50,0%	0	0,0%	1	50,0%
Castelo Branco	2	1	50,0%	0	0,0%	0	0,0%	0	0,0%	1	50,0%
Lisboa	35	5	14,3%	3	8,6%	10	28,6%	0	0,0%	17	48,6%
Aveiro	5	0	0,0%	0	0,0%	3	60,0%	0	0,0%	2	40,0%
Porto	25	2	8,0%	2	8,0%	12	48,0%	0	0,0%	9	36,0%
Setúbal	3	1	33,3%	0	0,0%	1	33,3%	0	0,0%	1	33,3%
Santarém	4	0	0,0%	1	25,0%	1	25,0%	1	25,0%	1	25,0%
Braga	4	1	25,0%	0	0,0%	2	50,0%	0	0,0%	1	25,0%
Coimbra	10	2	20,0%	1	10,0%	5	50,0%	1	10,0%	1	10,0%
Leiria	3	1	33,3%	0	0,0%	1	33,3%	1	33,3%	0	0,0%
Beja	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Évora	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Ponta Delgada	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Vila Real	2	0	0,0%	0	0,0%	2	100,0%	0	0,0%	0	0,0%
Faro	2	0	0,0%	0	0,0%	2	100,0%	0	0,0%	0	0,0%
Viseu	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Bragança	1	0	0,0%	0	0,0%	1	100,0%	0	0,0%	0	0,0%
Funchal	3	1	33,3%	0	0,0%	2	66,7%	0	0,0%	0	0,0%
Guarda	1	1	100,0%	0	0,0%	0	0,0%	0	0,0%	0	0,0%
Total:	**111**	**15**	**13,5%**	**7**	**6,3%**	**48**	**43,2%**	**3**	**2,7%**	**38**	**34,2%**

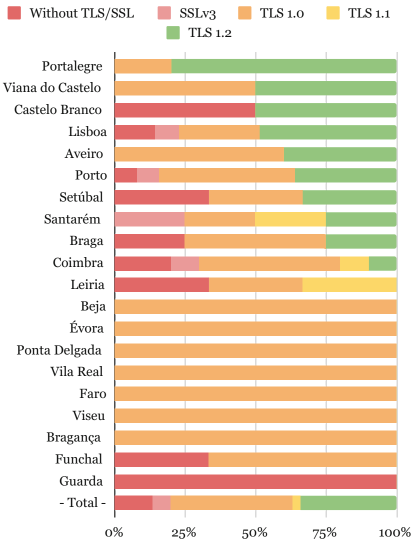

Fig. 8. Worst supported SSL/TLS Versions

negotiate at least on version TLSv1.0. Lastly, the districts of Lisboa, Porto, Santarém and Coimbra also have HEIs that negotiate on the SSLv3, representing 6.3% at a national level.

5 Conclusions

There are several security-related standards and recommendations concerning DNS and HTTP services. These standards and recommendations are relevant to enhance the security of public and private institutions. HEIs should also comply and be updated regarding these efforts to improve the security of their services and information, however, they present different statuses and paces in the adoption of these web-related security services.

This article presented an overview of the HEIs national panorama regarding the implementation of security-related standards and recommendations regarding DNS and HTTP services. A set of scripts were developed and data was collected namely regarding the support of DNSSEC, SSL certificates (including the respective CA), key size and algorithms used and SSL/TLS negotiations cyphers.

From the results obtained, it was verified that only 11.7% of HEIs support DNSSEC, in which 10% are public. Roughly 14.4% do not use any SSL certificates and those who support it, 18.9% do not force the usage. In regards to the CA used, the guidance is as follows: 28.8% of HEIs use *GEANT* as their CA, on private HEIs the most used CA is *Let's Encrypt*, totalling 11.7%, In regards to the SSL ciphers and algorithms, 74.8% of HEIs use a 2048 bits encryption key and 81.1% use the RSA algorithm. When it comes to SSL/TLS negotiations, 24.3% of HEIs already negotiate with the latest TLS version: TLSv1.3, while 6.3% of HEIs still negotiate with the vulnerable SSL version: SSLv3.

Future efforts of these HEIs should focus on (1) the adoption of DNSSEC, to add an extra layer of protection against DNS attacks and (2) implement correctly the HTTP redirection mechanisms and assure the support of the updated versions of SSL certificates to secure data communication between systems. In particular regarding SSL/TLS negotiation, the institutions that use SSLv3 are strongly encouraged to disable this protocol due to its vulnerability to man-in-the-middle attacks, and they should apply TLSv1.2 and TLSv1.3.

Acknowledgments. This work was developed in the context of a project in the Computer Networks and Systems Engineering graduation at the Instituto Politécnico de Viana do Castelo, Portugal, and it was partially supported by the Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (ERDF), within project "Cybers SeC IP" (NORTE-01-0145-FEDER-000044).

References

1. Direção Geral de Estatísticas de Educação e Ciência - Rede atual de Estabelecimentos do Ensino Superior. https://www.dgeec.mec.pt/np4/38/. Accessed 12 Apr 2021
2. EURYDICE - National Education Systems. https://eacea.ec.europa.eu/national-policies/eurydice/national-description_en. Accessed 1 July 2021
3. The top 500 sites on the web the sites in the top sites lists. https://www.alexa.com/topsites. Accessed 5 July 2021
4. Allen, C., Dierks, T.: The TLS Protocol Version 1.0. RFC 2246, January 1999. 10.17487/RFC2246. https://rfc-editor.org/rfc/rfc2246.txt
5. Chan, C.l., Fontugne, R., Cho, K., Goto, S.: Monitoring TLS adoption using backbone and edge traffic. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 208–213 (2018). https://doi.org/10.1109/INFCOMW.2018.8406957
6. Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346, April 2006. 10.17487/RFC4346. https://rfc-editor.org/rfc/rfc4346.txt
7. Elgamal, D.T., Hickman, K.E.: The SSL Protocol. Internet-Draft draft-hickman-netscape-ssl-00, Internet Engineering Task Force, April 1995. https://datatracker.ietf.org/doc/html/draft-hickman-netscape-ssl-00. Work in Progress
8. Freier, A.O., Karlton, P., Kocher, P.C.: The Secure Sockets Layer (SSL) Protocol Version 3.0. RFC 6101, August 2011. 10.17487/RFC6101. https://rfc-editor.org/rfc/rfc6101.txt
9. Incm: Resolução do conselho de ministros 92/2019 (2019). https://dre.pt/home/-/dre/122498962/details/maximized
10. Le, T., van Rijswijk-Deij, R., Allodi, L., Zannone, N.: Economic incentives on dnssec deployment: time to move from quantity to quality. In: NOMS 2018–2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–9 (2018). https://doi.org/10.1109/NOMS.2018.8406223

11. da República, A.: Lei 62/2007 (2007). https://dre.pt/web/guest/pesquisa/-/search/640339/details/normal?q=Lei. n. º 62/2007
12. Rescorla, E.: HTTP Over TLS. RFC 2818, May 2000. 10.17487/RFC2818. https://rfc-editor.org/rfc/rfc2818.txt
13. Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. 10.17487/RFC8446. https://rfc-editor.org/rfc/rfc8446.txt
14. Rescorla, E., Dierks, T.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, August 2008. 10.17487/RFC5246. https://rfc-editor.org/rfc/rfc5246.txt
15. Rescorla, E., Schiffman, A.M.: The Secure HyperText Transfer Protocol. RFC 2660, August 1999. 10.17487/RFC2660. https://rfc-editor.org/rfc/rfc2660.txt
16. Rose, S., Larson, M., Massey, D., Austein, R., Arends, R.: DNS Security Introduction and Requirements. RFC 4033, March 2005. 10.17487/RFC4033. https://rfc-editor.org/rfc/rfc4033.txt
17. Rose, S., Larson, M., Massey, D., Austein, R., Arends, R.: Protocol Modifications for the DNS Security Extensions. RFC 4035, March 2005. 10.17487/RFC4035. https://rfc-editor.org/rfc/rfc4035.txt
18. Rose, S., Larson, M., Massey, D., Austein, R., Arends, R.: Resource Records for the DNS Security Extensions. RFC 4034, March 2005. 10.17487/RFC4034. https://rfc-editor.org/rfc/rfc4034.txt
19. Song, Y.D., Mahanti, A., Ravichandran, S.C.: Understanding evolution and adoption of top level domains and DNSSEC. In: 2019 IEEE International Symposium on Measurements Networking (M N), pp. 1–6 (2019). https://doi.org/10.1109/IWMN.2019.8805011
20. Suga, Y.: Status survey of SSL/TLS sites in 2018 after pointing out about "search form" issues. In: 2018 Sixth International Symposium on Computing and Networking Workshops (CANDARW), pp. 483–485 (2018). https://doi.org/10.1109/CANDARW.2018.00093
21. Van Adrichem, N.L.M., Lua, A.R., Wang, X., Wasif, M., Fatturrahman, F., Kuipers, F.A.: DNSSEC misconfigurations: how incorrectly configured security leads to unreachability. In: 2014 IEEE Joint Intelligence and Security Informatics Conference, pp. 9–16 (2014). https://doi.org/10.1109/JISIC.2014.12
22. Weerasinghe, T., Disanayake, C.: Usage of RC4 cipher in SSL configurations in web portals of Sri Lankan banking/non-banking financial institutes and awareness levels of relevant staff about it. In: 2018 National Information Technology Conference (NITC), pp. 1–6 (2018). https://doi.org/10.1109/NITC.2018.8550064
23. Yee, P.E.: Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 6818, January 2013. 10.17487/RFC6818. https://rfc-editor.org/rfc/rfc6818.txt