Secure Browsing in Local Government: The Case of Portugal

Hélder Gomes[1,3,*], André Zúquete[2,3], Gonçalo Paiva Dias[1,4] and Fábio Marques[1,3]

[1]*Escola Superior de Tecnologia e Gestão de Águeda (ESTGA), Universidade de Aveiro, Portugal*
[2]*Departamento de Eletrónica, Telecomunicações e Informática (DETI), Universidade de Aveiro, Portugal*
[3]*Institute of Electronics and Informatics Engineering of Aveiro (IEETA), Universidade de Aveiro, Portugal*
[4]*Research Unit on Governance, Competitiveness and Public Policies (GOVCOPP), Universidade de Aveiro, Portugal*
E-mail: helder.gomes@ua.pt; andre.zuquete@ua.pt; gpd@ua.pt; fabio@ua.pt
[*]*Corresponding Author*

Received 25 September 2019; Accepted 07 April 2021;
Publication 10 June 2021

Abstract

This article addresses the adoption and use of Hypertext Transfer Protocol Secure (HTTPS) in the entry pages of the official websites of all (308) Portuguese municipalities. This is relevant because such websites are typically used to provide transactional services to citizens, and citizens need to trust that websites are authentic and that confidentiality and integrity of the information exchanged is assured in the communication process. Automated and, whenever needed, manual analyses were used to investigate the entry pages. Specifically, we checked for the existence of an HTTPS site; the correctness of website certificates and their certification chain; coherence between contents of the HTTP and HTTPS versions of websites; redirection from the HTTP version of a website to its HTTPS version; the existence of resources

Journal of Web Engineering, Vol. 20_4, 935–962.
doi: 10.13052/jwe1540-9589.2041

fetched using HTTP in HTTPS versions of websites; and exploitation of HSTS. A Quality Indicator was then defined and a classification of the municipalities into quality groups was produced. Possible determinants for the results obtained by the municipalities were also investigated. The general conclusion is that there is still much to be done to assure that citizens can communicate securely with the websites of all Portuguese municipalities, since only 3.6% of the municipalities were considered good, while 46.1% do not guarantee the minimum conditions. We argue that these results are associated with the fact that most Portuguese municipalities do not have the critical technical and managerial mass to correctly implement and maintain their websites. To mitigate this limitation, we propose the dissemination of technical instructions on how to correctly configure and deploy municipal HTTPS websites and the creation of shared services between the smaller municipalities.

Keywords: e-government, local government, HTTPS, privacy, confidentiality, security, Web.

1 Introduction

All Portuguese municipalities have an official website, which is the main reference point both for the provision of municipal services to the citizens and for the promotion of the municipality. Among the provided services, there are informational services, with information regarding municipal government bodies and municipal regulations and services, and transactional services that municipal citizens may obtain electronically. Trust is fundamental for the citizen's adherence to electronic services [1] in general and in particular to those provided by municipal websites. For that reason, municipal websites should authenticate to citizens, to ensure citizens they are contacting legitimate, official websites, and that the access to the information and services in municipal websites is confidential and correct. Note that confidentiality in communications was one of the top concerns pointed by citizens in a public consultation on the ePrivacy Directive Review [2].

The content of websites has been traditionally provided using the HTTP protocol. However, this protocol does not include any security feature, thus being prone to interception attacks (aka Man-in-the-middle attacks) and to service impersonation attacks. Consequently, in the last years there was a migration from HTTP to HTTPS [3], which is backed by standard bodies, such as the World Wide Web Consortium (W3C) [4] and the Internet Architecture Board (IAB) [5], and by major browsers [6, 7].

Despite some vulnerabilities [8] and some known weaknesses when used in e-government websites [9], HTTPS aims to provide authentication, integrity and confidentiality to the communication between a browser and a website, which is considered fundamental for a trustworthy interaction between municipal websites and citizens. Furthermore, the protection provided by HTTPS is in line with the "European Proposal for an ePrivacy Regulation" [10] – a proposal to adapt the privacy in electronic communications to the new European General Data Protection Regulation (GDPR) [11].

In this paper we extend the work in [12], where we presented the results of a survey on the adoption of HTTPS in the official websites of all (308) Portuguese municipalities, by adding a technical background on HTTPS, an analysis of related work (both presented in Section 2), a more detailed description of the methodology used throughout the study, including the methods to identify the determinants for the classification (which can be observed in Section 3), and an improved discussion of the results of the study and of its implications (which is presented in Section 5).

2 Background

In this section we provide a technical background on the HTTPS protocol and its features that makes possible a secure redirection from HTTP to HTTPS, followed by a review of related work.

2.1 Technical Background

A web page is identified by an URL (Uniform Resource Locator [13]), e.g. `http://www.cm-cityname.pt/page1`, which is composed of three parts. The first part identifies the protocol used to access the page ("`http://`" in the URL above); "`http`" is used for HTTP, whilst "`https`" is used for HTTPS. The second part is the DNS (Domain Name System [14]) name of the machine where the page is located ("`www.cm-cityname.pt`" in the URL above). Finally, the third part is the location of the page in the machine ("`/page1`" in the URL above).

DNS names allow humans to identify computers based on names, as we are not good at handling Internet Protocol (IP) addresses (the identifiers of computers on the Internet). DNS names are hierarchical, from right to left, starting from a top domain (the "." (dot) domain often implicit in DNS names) and going into inner subdomains. For example, we can read the DNS name in the URL above as the "`www`" sub-domain (machine name) in the

"`cm-cityname`" subdomain (organization) in the "`pt`" subdomain (country). Having names easily associated with the owner entities is important for people to memorize and to better recognize the organization owning the name.

On the Web, services are provided by web servers (the computers identified by DNS names) and are typically obtained using web browsers, using the HTTP protocol or its secure variant, HTTPS. Guaranteeing the quality of an HTTP user-service requires a multi-technological approach.

First of all, it requires proofs of authenticity of all the contents presented on behalf of the service. These proofs, provided by the service, usually cannot be checked by humans. They are cryptographic evidences that the presented contents came from the intended sources (which may be more than the requested web service). These proofs are supplied by the TLS (Transport Layer Security [15]) protocol used within an HTTPS interaction, but they depend, in the first place, on the service authentication performed during the setup of a TLS session. This authentication usually uses X.509 certificates, which bind a cryptographic key to the service's DNS name. It is this bound, as well as the correctness of the certificate, that proves to a browser (and, transitively, to its user) that it is interacting with the intended service.

The correctness of a certificate is checked with a multi-step verification of the correctness of its certification chain, which is a sequence of (intermediate) certificates of Certification Authorities that provide a trustworthy correctness assurance from a trusted root certificate. This root certificate is necessarily known, and trusted, by the verifier. Therefore, during the setup of a TLS session, the server-side should send not only its certificate, but also the certification chain from a well-known root certificate, to allow clients to be able to validate its certificate. A failure in the provisioning of intermediate certificates of the certification path may, or may not, raise a validation exception on the verifier. If the verifier already knows, from past activity, the missing intermediate certificates, it can fill the gaps and succeed on the verification. Otherwise, it fails, and service authenticity cannot be asserted.

Since the correctness of the contents presented by a web service can only be assured with TLS (thus, with HTTPS, which is HTTP on top of TLS), responsible web services should never respond to HTTP requests, but solely to HTTPS requests. However, this is not enough for stopping a powerful attacker from misleading users.[1] In fact, such an attacker can block the users' path to the HTTPS service and provide, by itself, a fake HTTP interface for

[1] For instance, using sslstrip (https://moxie.org/software/sslstrip).

the same service, possibly forging some of its contents. There is no easy solution for this other than to adopt the so-called HTTPS-only strategies. In one part, this strategy requires clients not to accept HTTP interactions instead of HTTPS if they know that the service is solely provided by HTTPS (e.g. using ForceHTTPS [16] or similar strategies). However, this strategy is hard to enforce by humans if a given set of similar services is not globally and coherently provided through HTTPS.

Besides relying on humans to enforce HTTPS-only access policies, there are a couple of mechanisms that can be used to assist users in such task: correct **HTTP redirections** and **HSTS** (HTTP Strict Transport Security [17]).

HTTP is a resource request protocol: the client (browser) requests a resource; the server (web service) sends the resource with a success code (200) or some other code to signal an exceptional event. Among all possible codes, we have the so-called **redirection codes**, in the range 300-399 (or 3XX for short). These codes are used to inform the requester that the target resource moved, and along with them is provided the actual location of the resource. These redirections are usually transparent to users, since browsers do not report them; therefore, users are not aware they actually exist.

HTTP redirections can deal with different resource relocation scenarios. Among them, we have temporary and definitive relocations. Temporary relocations should not be memorized by browsers, as they may disappear in the future. Definitive relocations, on the other hand, can be memorized by browsers to avoid losing time with future redirections. Therefore, services willing to help browsers to follow an HTTPS-only strategy, should respond to any HTTP request with a redirection to that same service but using HTTPS; and the return code must be 301 (Moved Permanently). Note that a powerful attacker may prevent these redirections to reach the client, and forge the web service, but a browser with this redirection memorized will never be fooled.

HSTS is a mechanism that a web service can use to instruct a browser to use solely HTTPS for accessing resources of the same domain or subdomains [17, 18]. When a resource with a name starting by "`https://company.tld`" is accessed, if the reply contains an HSTS indication (in an HTTP header field), then all subsequent accesses to resources under domain "`company.tld`" need to be done through HTTPS. Furthermore, such indication can be extended to subdomains, which would affect resources such as the ones in the domain "`www.company.tld`". Finally, the HSTS indication has a lifetime, which is refreshed each time the resource is accessed.

The HSTS mechanism also leads browsers to enforce a very strict policy regarding the validation of certificates provided by web services affected by HSTS. In fact, any failure in the validation of such certificates will be assumed as evidence of an attack being performed, and not as a server misconfiguration. As such, the browser should not give the user a chance to proceed.

Complementary, most browsers today follow a trend created by Chrome of using a list of preloaded domains adhering to HSTS [19, 20]. This list can be increased by other domains by using the preload indication in their HSTS header field.

Continuing to consider how to ensure the quality of the web contents presented to users, one critical issue is the rendering of a web page using contents fetched with both HTTP and HTTPS, thus creating the so-called **mixed content**. Mixed content can be particularly dangerous when active content (JavaScript) is fetched with insecure connections, but it can also be dangerous when passive content is at stake (HTML, CSS, images, movies, etc.). According to [20], major browsers forbid mixing active contents, but only (visually) warn against mixed passive contents.

Content Security Policy (CSP) is a not-yet standard approach for providing browsers with several types of security policies regarding the contents they fetch and handle. CSP allows an HTTP resource to refer to the requester that it should be fetched with HTTPS (upgrade secure requests feature). CSP can also be used to limit the locations of resources used to render a web page, a feature that is particularly effective in preventing XSS (Cross-Site Scripting) attacks [21]. And CSP can be used to instruct a browser not to allow mixed contents in the handling of the contents of an HTTPS resource. In such cases, browsers will just disregard HTTP fetched resources and produce error messages in their console, which users rarely check (or even know about). Therefore, although CSP may protect users, it is more useful for evaluating the correctness of HTTPS web pages, in terms of mixed contents, during their development.

Wrapping up, a proper web service configuration, which ensures the authenticity (and the secrecy) of the contents provided to users with the help of their browser, must:

- Provide an HTTPS web service;
- Use a valid certificate to authenticate the HTTPS web service;
- Provide a complete intermediate certification path for validation of the HTTPS web service certificate;

- Provide an HTTP web service that uses HTTP redirections 301 (Moved Permanently) to HTTPS resources;
- Include HSTS indications in the header of HTTPS responses; and
- Web pages provided by an HTTPS web service should not use mixed contents.

2.2 Related Work

One of the difficulties for general HTTPS adoption is the cost of certificates and the manual process for its installation. Let's Encrypt aims to solve this problem by issuing free certificates for web servers and automated deployment. The study conducted by [22] tried to determine the adoption pattern of the certificates issued by Let's Encrypt. The study used Certificate Transparency Logs and other sources such as Alexa's[2] historic records, geolocation databases and VirusTotal, from October 2015 to May 2016, to determine the acquisition and usage of the certificates issued by Let's Encrypt. As a result of this study, the authors found that 46% of sites owning Let's Encrypt active certificates are not using them. Also, they found that 15% of all issued certificates have not been renewed.

Previous studies have addressed the usage of HTTPS, namely regarding its adoption [23–33] including the increase of HTTPS traffic [27, 30], and the quality of the implementation at server-side [18, 23–26, 28, 29, 31–34]. However, only one of these studies is targeted to the specific domain of local e-government, in Sweden [24], and none of them explores the determinants of the adoption. Next these papers are detailed.

Two studies conducted by [23] and [26] in 2013 and 2015, respectively, evaluated the adoption of client-side security mechanisms in websites of European Union countries. In the first study, more than 22000 websites were analysed for vulnerabilities and weaknesses (such as, mixed content inclusion, Weak Browser XSS Protection or outdated server software) and for countermeasures (e.g. HSTS, CSRF Tokens or HTTPOnly Cookies). The authors found that only 5113 websites had at least one page delivered over HTTPS and that more than 80% of the websites had content provided by unsecured sources. The second study was divided into three categories: Secure Communication, Cross-Site Scripting and Secure Framing. In the Secure Communication category, authors verified if the website supports HTTPS connections and the use of HSTS policy and secure cookies. It

[2] https://www.alexa.com/

was found that approximately 32% of the 18000 websites used HTTPS, an increase of more 2383 websites since 2013, and an increase of about 4% on the use of HSTS.

Another study [24] was carried out in Sweden to assess the websites of local government regarding the implementation of GDPR. The authors developed a five-step scoring system and developed two tools: one to check the individuals' privacy and the other to check the websites of the municipalities. The authors found that no municipality is ranked in the two higher scores of their five-step scoring system. In addition, some suggestions were made by the authors for the implementation or adaptation of municipal sites. In terms of the adoption of HTTPS, in the latter assessment (August 20, 2016) they found that only 19 out of 290 municipalities used HTTPS.

In [25], a security analysis was made to the 1 million websites of the Alexa rank, with data collected in January 2016. Among other results, the authors quantified the impact of trackers and third parties on HTTPS deployment. They found that only 8.6% of the top 1 million websites are HTTPS only. From these, they found that 7.75% of websites load with mixed content warnings, meaning they are loading content from non-HTTPS sources.

In [27], the authors used the telemetry of Google Chrome and Firefox browsers to analyse the adoption of HTTPS. This analysis concluded that the adoption of HTTPS continues to increase, that the use of HTTPS differs geographically and with the operating system used.

In another study [28], the exposure of web servers and HTTP security headers to attackers was evaluated on a set of 240 websites from Mozambique. The study revealed that only 6% of the websites do not use HTTP (HTTPS only) and that 62% have both HTTPS and HTTP. More, they found that 22% of the HTTPS websites used self-signed certificates.

In [29], the authors presented an application, Dmap, to reduce the complexity of executing both measurements and analysis on what they refer to as a DNS ecosystem, the set of entities/companies responsible for delivering the various services behind each Internet domain name. It does so by automating the crawling of several application protocols, including HTTP(S), and by storing the results into a relational database. The tool was used to profile the Alexa 1 million websites, in January 2018, and found that 77,2% of those domains use HTTPS and, from those, 21.4% use Let's Encrypt certificates. Also, they found, by comparing data from two measurements on the "`.nl`" (Netherlands) domain, in September 2017 and February 2018, that the use of self-signed certificates is reducing.

In [30], the authors monitored a set of protocols, including HTTP, and their use with TLS. The data which was analysed was acquired from January 2008 to August 2017 on a backbone and an edge academic network in Japan. HTTPS usage increased over the years: in the backbone it increased from 4% in 2008 to 36% in 2017, and in the edge academic network it increased from 50% in 2014 to 65% in 2017. Interestingly, they found that the increase in HTTPS traffic is associated with the HTTPS adoption by major web companies. Despite these figures, HTTPS adoption is still low compared to the use of TLS on other protocols.

Another study was made by [31] using data collected in September 2017 from the websites in the Alexa rank of 1 million domains. They found that only 47.7% of the HTTPS websites were properly configured. They also found that HSTS was implemented only in 17.5% of the HTTPS websites and that only about 2% of the HTTP websites redirect to an HTTPS website while simultaneously enforcing HSTS policy.

Robinson, in [32], provided a study that compares the implementation of HTTPS on the websites of urban and rural hospital in Illinois. Although there is sensitive information that can be obtained by site navigation, about 76% of the 210 websites had adopted HTTPS, but only 54% of them had a Grade A classification (according to the classification of Qualys[3]). Of these, 40% belonged to websites of rural hospitals and the remaining ones to websites of urban hospitals.

In [33], the authors presented an analysis of the adoption of HTTPS on the 241 Hellenic websites listed on Alexa's rank. Their focus was on a set of TLS vulnerabilities (such as the use of the RC4 cipher, if it was vulnerable to the Heartbleed attack and/or if they were vulnerable to the Drown attack). They stated that the adoption of HTTPS on Hellenic websites was not adequate. In fact, they determined that about 3% of the websites did not implement HTTPS on pages that provide a login procedure. There were also several problems detected related to the vulnerabilities of TLS, which led them to conclude that about half of the websites must improve their TLS configurations.

In [34], data from the Alexa 1 million domains, collected in October 2013, was used to evaluate the state of HTTPS deployment, having the authors found a significant number of web servers sending an HSTS header. However, many of these web servers do not secure their subdomains, leaving them open to many attacks that HSTS was meant to mitigate.

[3]https://www.qualys.com

While conducting an HTTPS adoption study on websites, such as most of the above-mentioned work, our study focuses on the specific local e-government domain in Portugal. Our goal is to characterize the adoption of HTTPS by Portuguese municipalities in order to raise awareness of the risks of not adopting HTTPS. Also, we classify municipalities according to a Quality Indicator and we try to identify possible determinants for the classification obtained by municipalities.

3 Methodology

3.1 Tools and Data Acquisition

The URLs of all the 308 municipalities were collected from the website of *Associação Nacional de Municípios Portugueses* (ANMP), the national association of Portuguese municipalities. Five of them were found to be wrong, and the correct URL was searched with Google. All URLs have an HTTP anchor, instead of an HTTPS.

Most URLs contain a DNS name that follows a homogeneous and straightforward structure: "`www.cm-name.pt`", where name is a diacritic-free abbreviation of the municipality name (e.g. "`fozcoa`" for Vila Nova de Foz Côa, "`vrsa`" for Vila Real de Santo António). No fixed rule exists for the abbreviations used, but they are not unnatural.

There are 38 exceptions to the default naming strategy (12.3%). Among them, there are two municipalities whose DNS names are under the "`.com`" domain: Santana ("`www.cm-santana.com`") and Oliveira de Frades ("`www.cm-ofrades.com`").

From 12 to 20 November, 2018, we conducted a series of automated analysis to all those URLs, using several tools and resorting to manual analysis with a browser only when necessary. Only the entry pages of municipal websites were accessed during this evaluation. No crawling was made throughout other pages accessible from those. Also, we did not assess the quality or the strength of the cryptographic algorithms, the presence of well-known SSL/TLS vulnerabilities, or even websites' vulnerabilities, since that would introduce more layers of entropy in an assessment that we want as simple as possible.

We used the gnutls-cli tool to check the presence of HTTPS sites (default 443 TCP port) and to extract their certificate and certification chain. We used the result of gnutls-cli certificate validation and we also developed a small Java program to validate the certificates, which was run using OpenJDK root

trust anchor certificates and using Debian Linux root trust anchor certificates. Both strategies produced the same result.

We used the wget tool to learn the HTTP redirections (HTTP codes 3xx) returned within the access to those web pages, both using HTTP and HTTPS. Finally, this tool enabled us to assess the usage of HSTS by the municipalities' main web page.

Finally, we used the OpenWPM tool [25] to confirm the HTTP redirections and the usage of HSTS, to obtain snapshots of entry web pages, both provided through HTTP and HTTPS, and to trace the resources accessed by the main web page of all municipalities in order to assess the uniform protection of all the resources accessed through those pages (namely, if there were resources accessed through HTTP from a web page accessed through HTTPS). This tool also enabled us to clarify the access to some web pages that refused to provide resources to wget.

3.2 Overall Quality Indicator

To classify and rank websites according to the quality of the implementation of HTTPS, the results of the municipalities were resumed in a Quality Indicator, presented in Table 1, with four classification levels:

- **Good:** the municipal website has a correct HTTPS web entry page that uses no HTTP resources, HTTP access is redirected to HTTPS using code 301 and HSTS is enforced.
- **Reasonable:** the municipal website has a correct HTTPS web entry page that uses no HTTP resources.
- **Minimum:** the municipal website has a correct HTTPS web entry page.
- **Bad:** None of the previous cases.

By correct HTTPS web page we mean that the web server certificate is valid, the content fetched through HTTPS is equal to the one obtained through HTTP and there is no HTTPS to HTTP redirection.

3.3 Determinants Identification

In order to identify possible determinants for the classification of the municipalities according to the Quality Indicator, we run multiple independent T-tests to identify significant mean differences between groups of municipalities. The tests were performed for three dichotomous dependent variables that are based on combinations of the indicator's classes: 'good'; 'good or

Table 1 Quality indicator

	Good	Reasonable	Minimum	Bad
HTTPS Service (TCP port 443)	Yes	Yes	Yes	
Valid Certificate with Cert. Chain	Yes	Yes	Yes	
HSTS and Redirection to HTTPS (Code 301)	Yes			
HTTPS page include HTTP Resources	No	No		
No HTTP page or equal HTTPS and HTTP pages	Yes(1)	Yes(2)	Yes(2)	
Redirection to HTTP	No	No	No	

(1) Only an HTTPS page exists
(2) Either only an HTTPS page or equal HTTPS and HTTP pages exist.

reasonable'; and 'good, reasonable or minimum'. As independent variables we selected four indicators:

- The variables 'municipal taxes' (logarithmized) and 'school dropout rate', because they were identified in [35] as relevant predictors of local e-government sophistication in Portugal;
- The variables 'total population' (logarithmized) and 'population density' (logarithmized), because they were identified as relevant predictors of local e-government sophistication in several international studies (for example [36, 37]);

Additionally, 'local e-government maturity' was also selected to be tested as an independent variable envisioning to investigate a possible relation between the level of security offered and local e-government sophistication. Data from a previous study on e-government maturity of all Portuguese municipalities was used for this purpose [38]. The other indicators were obtained from the National Statistics Institute and are relative to 2017.

Finally, we run logistic regressions to investigate to what extent the independent variables for which significant mean differences were found can be used as predictors of the classifications obtained by municipalities or, in other words, obtain a measure of the part of the phenomenon that is explained by the variability of those variables.

4 Results

4.1 Descriptive Analysis

In this section, we will describe the analysis that we did to the provision of the entry web page of Portuguese municipalities through HTTPS.

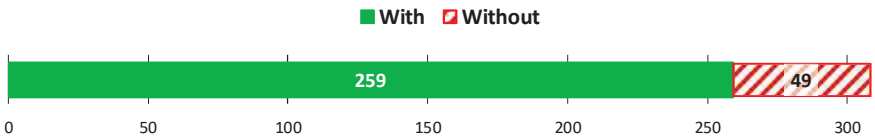


Figure 1 Number of municipalities with and without a TLS server on port 443.

4.1.1 Municipalities with an HTTPS web server

Through an automated analysis using gnutls-cli and wget we concluded that 259 municipalities (84.1%) have a server on port TCP 443 that is able to initiate a TLS session (Figure 1) and, possibly, provide the main web page through HTTPS. However, not all those municipalities provide their main web page through that server. The analysis of the characteristics of the service provided on TCP port 443 is the focus of this descriptive analysis section.

4.1.2 Certificate provided by municipal web servers

Through an automated analysis using gnutls-cli we extracted the certificate of all municipal HTTPS servers and analysed their correctness. By correctness, we mean:

- A server certificate must have the DNS name of the website or a wildcard DNS name in the Subject field or in the Subject Alternate Name field (e.g. "`*.cm-albufeira.pt`" for all DNS names belonging to the DNS domain "`cm-albufeira.pt`");
- A server certificate must be provided together with a complete and correct certification chain (excluding the root certificate);
- A server certificate cannot be self-certified;
- A server certificate or any certificate of its certification chain cannot be expired.

In all these cases, a browser blocks access to the server and presents an error message that gives some details about the problem encountered. However, a typical user would not be able to understand the error and browsers typically suggest users not to proceed in the access to the problematic server in order to avoid problems.

Only 178 municipalities (57.8%) presented a correct certificate, and 81 (26.3%) presented a wrong certificate (Figure 2). The breakdown of the problems found in those 81 municipalities is the following (note that there is an overlap in the numbers since some servers have more than one problem):

- 71 (87.7%) do not have the website DNS name in the server certificate;
- 7 (8.6%) do not provide a complete certification chain;

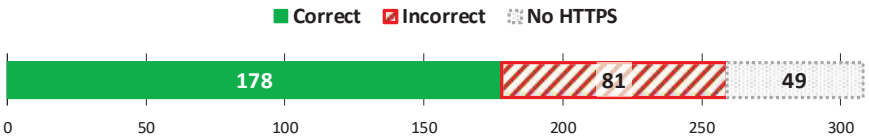


Figure 2 Number of municipalities with correct and incorrect certificates for their HTTPS server.

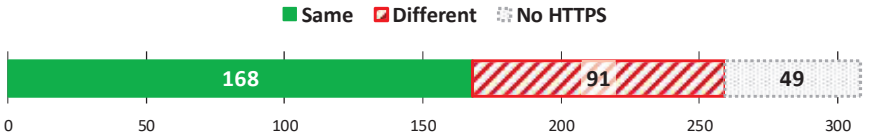


Figure 3 Municipal websites that provide the same and different content with HTTP and HTTPS.

- 27 (33.3%) have a self-certified certificate;
- 20 (24.7%) have an expired certificate (16 of them are self-certified as well).

4.1.3 Content provided by HTTPS servers

The content provided by the HTTPS servers was compared against the content provided by the corresponding HTTP servers using the wget tool and screenshots captured with OpenWPM. Where it was not possible, or a mismatch was detected, manual observation was used. For this analysis, we specifically required the browser to ignore the correctness of servers' certificates, in order to get to the contents provided by HTTPS servers with a defective certificate setup. Also, to obtain the HTTPS pages correctly rendered we disabled the insecure contents protection in the browser.

From the 259 HTTPS web servers, 91 (35.1%) provide wrong content (Figure 3). Some notable cases are one municipality which provides the contents of the *Amigos de Deus* (God's Friends) website and two municipalities which provide the contents of the *Centro Hospitalar do Porto* (Porto's Hospital Centre) web page.

4.1.4 Exploitation of HTTP within resources fetched through HTTPS

HTTP resources, namely HTML pages, use external resources to help to compose the contents presented to a user (JavaScript code, CSS styles, images, movies, audio, etc.). Resources accessed through HTTPS should not use other

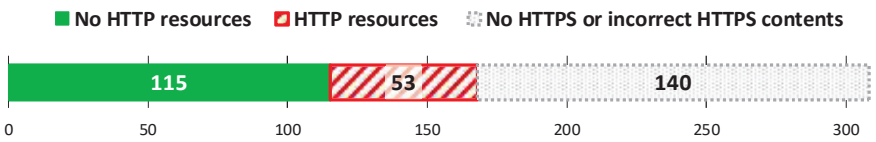


Figure 4 Use of HTTP resources in websites with correct HTTPS content.

resources fetched with HTTP, as this may create a security breach (as those resources may be tampered by an attacker with the power to intercept the communication between the browser and the server providing the unprotected resource). Only 115 (68.5%) of the 168 HTTPS web servers of municipalities that provide correct contents do not provide resources referring to other resources accessible through an HTTP URL (Figure 4).

4.1.5 Redirection between HTTP and HTTPS

Web servers of municipalities should use only HTTPS and should redirect all HTTP accesses to a corresponding HTTPS access (something known as HTTPS-only access). Redirections can be made with different HTTP redirection codes (3xx codes), but the advice is to use the 301 (Moved Permanently), because it gives browsers an indication to cache the redirection for future use, thus saving redirections.

There are, however, some other redirection mechanisms, such as using a refresh operation on a meta tag or using JavaScript code within an HTML web page. These methods may lead to the exact same result of an HTTP redirection but they are more difficult to assert, because they imply the parsing of downloaded HTML pages and JavaScript files. Since we restricted our analysis to the meta-information of municipalities' entry web pages, we were not able to get an accurate account of those redirections. Thus, for this analysis, those municipalities were by default accounted as not having an HTTP to HTTPS redirection. However, from other evidence, such as network traffic created by the entry pages, we found one municipality that uses content-embedded redirections and we counted it as having a redirection.

Only 103 (61.3%) of the 168 HTTPS servers that provide correct contents redirect HTTP accesses to their main web page to HTTPS (Figure 5). Within these (Figure 6), 76 (73.8%) use the HTTP code 301 and 27 use other codes: 302 (Found), 303 (See Other) or 307 (Temporary Redirect).

On the other hand, HTTPS to HTTP redirection constitutes a security downgrade and is not justifiable from a security point of view. However, 13 of all HTTPS servers (5.0%) redirect HTTPS to HTTP, and 5 of them use the HTTP code 301 to do so.

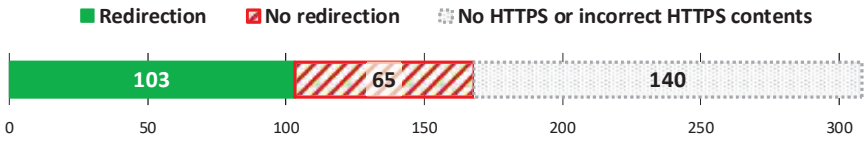


Figure 5 Redirection of HTTP entry page to HTTPS.

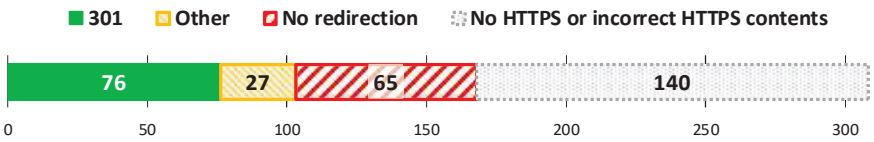


Figure 6 Redirection codes used for the redirection of HTTP entry page to HTTPS.

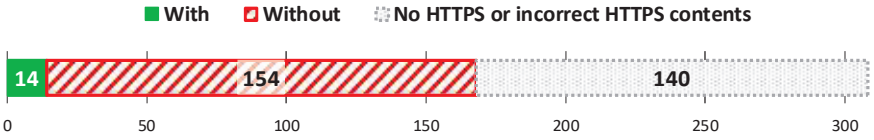


Figure 7 Usage of HSTS in websites with correct HTTPS content.

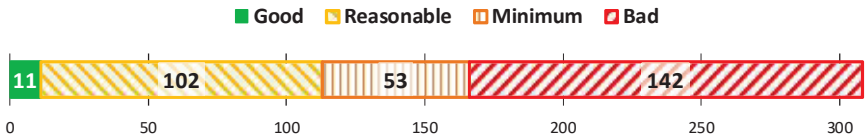


Figure 8 Classification of Portuguese municipalities regarding HTTPS usage.

4.1.6 Exploitation of HSTS

HSTS is a mechanism that HTTPS servers can use to force the usage of HTTPS by default to access all resources they provide. Servers convey this indication to browsers through an HTTP response header field (Strict-Transport-Security). Only 14 (8.3%) of the 168 HTTPS servers that provide correct contents use HSTS (Figure 7).

4.2 Classification of Portuguese Municipalities

Using the Quality Indicator presented in Table 1, the Portuguese municipalities classify as follows (Figure 8): 11 Good (3.6%), 102 Reasonable (33.1%), 53 Minimum (17.21%) and 142 Bad (46.1%).

4.3 Paradigmatic Cases

Some paradigmatic cases illustrate how confusion can create abnormal and dangerous situations. One municipality (here referred to as mname) uses two different domains, "`mname.pt`" and "`cm-mname.pt`". All HTTP accesses to both domains (using either the domains' name or its www host) redirects to an HTTPS server at "`mname.pt`". However, direct accesses to the www HTTPS server in both domains ("`www.cm-mname.pt`" or "`www.mname.pt`") or even to "`cm-mname.pt`" yield a defective server configuration (with a wrong certificate owned by another municipality).

Other paradigmatic cases are municipalities that have an HTTPS web server but redirect the incoming requests to HTTP. This is incomprehensible since they voluntarily use protected access to abandon it in favour of unsecured accesses. Furthermore, some servers use code 301 (Permanent Redirection) to perform the downgrade, which indicates browsers that HTTPS is not to be used in future accesses to them.

Some municipalities classify as bad because of a small, but relevant, technical detail: the HTTPS server does not send the complete certification chain for its certificate. This can create a problem on client browsers as it may raise the "unknown certificate issuer" error, in the absence of the intermediate certificates. Such absence depends on the popularity of the intermediate certificates in other certification chains, so this problem may occur or not depending on the past actions of the client browser.

4.4 Determinants of Results

As explained in Section 3, we run multiple independent T-tests in order to identify possible determinants for the classification of the municipalities according to the Quality Indicator. Three dichotomous dependent variables were used: municipalities classified as 'Good'; municipalities classified as 'Good or Reasonable'; and municipalities classified as 'Good, Reasonable or Minimum'. Four indicators were used as independent variables: 'municipal taxes' (logarithmized); 'school dropout rate', 'total population' (logarithmized); 'population density' (logarithmized); and 'local e-government maturity'.

Table 2 shows the results of the significant T-tests (equal variance not assumed based on the previous Levene's test). Results for the statistically non-significant tests ($p > 0.05$) were omitted for simplicity. It turned out that there are significant mean differences only between the group of

Table 2 Results of the T-tests (only significant tests are presented)

Dependent Variable	good or reasonable		
Independent variables	Sig.***	Mean dif.	Std. err. dif.
Municipal taxes (log)	0.030*	−0.1623	0.0742
Total population (log)	0.007**	−0.1607	0.0592

*$p < 0.05$; **$p < 0.01$; ***Two extremities.

Table 3 Results of the binary logistic regression

Dependent Variable	good or reasonable			
Independent variables	B	Std. Err.	Sig.	Exp(B)
Municipal taxes (log)	0.818	0.651	0.209	0.441
Total population (log)	1.697	0.813	0.048*	4.989
Constant	−4.487	1.442	0.002**	0.021

*$p < 0.05$; **$p < 0.01$.

municipalities that have a classification of 'Good or Reasonable' and those that have a classification of Minimum or Bad. The significant mean differences for these two groups were obtained for the variables 'municipal taxes' and 'total population' (both logarithmized). For the remaining variables ('school dropout rate', 'population density', and 'local e-government maturity') no significant mean differences were found. In other words, the group of 'Good or Reasonable' municipalities is statistically different from the group of 'Minimum or Bad' municipalities when 'municipal taxes' and 'total population' are used as indicators.

To further investigate if those two independent variables can be used as predictors for a municipality to be classified as 'Good or Reasonable' we run a binary logistic regression using 'Good or Reasonable' as the dichotomous dependent variable and 'municipal taxes' (logarithmized) and 'total population' (logarithmized) as independent variables (the variables for which significant mean differences were found). The results are shown in Table 3. The model is statistically significant ($p < 0.05$) but it explains only 3.9% (Nagelkerke R^2) of the variance in the classification of municipalities and correctly classifies only 64.0% of the cases. The indicator 'total population' (logarithmized) is the only significant predictor in the model ($p < 0.05$). This suggests the existence of other relevant explanatory factors besides the ones that were tested in this study.

5 Discussion

In this section we discuss the results of the study (main risks, impact on citizens' trust, and determinants) and address their ethical concerns and limitations.

5.1 Risks and Citizens' Trust

Due to their nature, the weaknesses identified in this study cannot be exploited to jeopardize the servers of the municipalities or their contents. They can, however, be exploited by third parties to observe communication between citizens and the municipalities and to deceive citizens by impersonating the municipal websites. Indeed, relating the first, the use of non-encrypted communication (as is the case with HTTP) allows a 'man-in-the-middle' to observe and understand the information being exchanged. This puts at risk the privacy of citizens and the confidentiality of the information exchanged, either being it originated by the citizen or by the municipality. Relating the second, the inexistence of a secure authentication of the website (as is the case when HTTP is used or when HTTPS is used without a valid certificate) allows someone to deploy a false municipal website, which can be perceived as legitimate by the citizens. Besides having access to all the information exchanged, thus compromising privacy and confidentiality, the impersonator can provide false information to the citizen, possibly also compromising his security.

But probably the most important consequence of the identified vulnerabilities is the impact that they can have on citizens' trust. Indeed, if citizens in general became aware that their privacy, the confidentiality of their information or even their safety might be at risk, they will tend to avoid using municipal e-government services and thus compromise all the investment and efforts in developing such services. Besides trust in technology, trust in government could also be affected. Thus, action is urgent. If, once identified by this study, the vulnerabilities can be easily and quickly resolved, regaining citizens' trust can be a much more complex and time-consuming process.

5.2 Determinants of the Results

When the Quality Indicator is used, the results obtained by municipalities are associated with their dimension. Indeed, as previously presented, the group of 'good or reasonable' municipalities is statistically different from the group of 'minimum or bad' municipalities when 'municipal taxes' and 'total

population' are used as indicators. However, this association only explains a very small part of the phenomenon.

Although, due to the methods used, no direct proof can be provided, this existing but relatively weak association of the results with the dimension of the municipalities might be resulting more from an indirect relation than from a direct one. Indeed, it might be the case that results be directly associated with the technical and managerial capacity of the municipalities and thus, indirectly, with their dimension, which would rationally explain the results. If this is the case, then the fact that most Portuguese municipalities are rather small and consequently might not have the critical mass to correctly implement and maintain their websites can be a serious handicap.

5.3 Ethical Concerns

As stated before, the weaknesses identified in this study can be exploited to compromise confidentiality of communications and the privacy and security of citizens. Thus, the disclosure of its results raises some ethical issues. Taking this into consideration, we formally notified the National Association of Portuguese Municipalities (ANMP – *Associação Nacional de Municípios Portugueses*) and the National Cybersecurity Centre (CNCS – *Centro Nacional de Cibersegurança*) of the results, previously to publication of the study. The information provided included a detailed list of all the vulnerabilities identified for each municipality. In addition, a time-lapse of almost three months between that notification and the submission of the study for publication was granted in order to allow time for the municipalities to take adequate measures in order to solve their vulnerabilities. Following this initiative, we also made a presentation of the study in an event organized by CNCS for a municipal technical audience. Some post-submission observations show that these actions have actually had an effect, with at least some municipalities solving the identified vulnerabilities.

5.4 Limitations of the Study

While not calling into question the findings of the study, there are some limitations associated with the used methods that must be addressed.

First, the study focused on the analysis of the official websites of Portuguese municipalities. Nevertheless, in order to avoid causing problems to the performance of the analysed sites, only the entry pages of the websites were accessed. Thus, it can well be argued that the results respect those

specific pages and not to the entire websites of the municipalities. However, it is also true that the existence of weaknesses in the entry pages might compromise the security of the hole websites, and even other websites of the same domain, for example through impersonation. On the contrary, the fact that there are no weaknesses in the entry page does not guarantee that all the website, or other websites in the same domain, are correctly deployed. It is, however, an indication that the municipality is aware of the need to implement the appropriate settings, or at least knows how to do it.

Second, besides comparing the similarities between pages available both through HTTP and HTTPS, we have not analysed the contents of the fetched web pages. Our focus was on the determination of the protocol (HTTP or HTTPS) used to fetch all the resources that compose the accessed pages. Therefore, we have not analysed other characteristics of web pages that may represent additional risks, like the use of third-party resources, the use of cookies, and the presence of trackers.

Third, we only analysed the offer of HTTPS in the municipal websites and the best practices in terms of technology used. We have not assessed the quality of the implementation of HTTPS websites in terms of the existence of known vulnerabilities or the usage of deprecated versions of protocols, which, of course, are of vital importance for the security of both users and municipal web servers.

6 Conclusions, Implication and Future Work

There is much room for improvement in order to ensure that all the websites of the Portuguese municipalities offer the necessary conditions for citizens to communicate securely with them. This is especially important because such websites are typically used to provide transactional services to citizens and citizens need to trust that the confidentiality of the information they submit is assured in the communication process. In a global classification, only 3.6% of the municipal web pages offer good security conditions, 33.1% offer reasonable conditions, 17.1% offer minimum conditions, and 46.1% offer bad conditions (meaning that they do not offer an HTTPS web page with a valid certificate). There is urgency in improving these results, not only to avoid the possible exploitation of the weaknesses identified, but also to prevent a loss of citizens' trust in the e-government services provided.

These results seem to be associated with the fact that most Portuguese municipalities are rather small and consequently might not have the critical technical and managerial mass to correctly implement and maintain their

websites. To mitigate this limitation, we propose the creation of shared services between small municipalities and the publication and dissemination of technical instructions on how to correctly configure and deploy municipal HTTPS websites. In any case, an important first step towards those directions is to raise awareness of the problem. It is important to note that we have not received any feedback from the ANMP, which lead to the conclusion that it is important to target the awareness messages not only to the technical community but also to the managerial community.

The results from this study are important and can be useful both for the technical and scientific communities. However, it does not exhaust the subject. Taking into account the identified limitations of this study, some future courses of action include: (i) to extend the analysis performed to include the identification of other types of weaknesses (e.g. content of fetched pages, use of third-party resources, use of cookies, presence of trackers, use of deprecated versions of protocols); (ii) to deepen the analysis to include all pages of the official websites and, whenever present, other websites in the same domain. Additionally, it will be interesting to (iii) apply the same methods in other countries or regions, or to other sectors, in order to allow for comparative studies; and (iv) to perform longitudinal studies by tracking the evolution of quality over time and relating it to public awareness of the problem and the adoption of specific policy instruments, such as the proposed creation of shared services and the dissemination of technical instructions.

Acknowledgement

This work was partially funded by National Funds through the FCT – Foundation for Science and Technology, in the context of the project UID/CEC/00127/2019.

References

[1] S. E. Colesca, "Understanding Trust in e-Government," *Inzinerine Ekonomika-Engineering Economics(3)*, no. 3, pp. 7–15, 2009.

[2] "ePrivacy: consultations show confidentiality of communications and the challenge of new technologies are key questions," *European Commission*, 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-

communications-and-challenge-new-technologies-are. [Accessed: 27-Nov-2018].

[3] C. Gupta, "The Market's Law of Privacy: Case Studies in Privacy and Security Adoption," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 78–83, 2017.

[4] M. Nottingham, Ed., "Securing the Web: W3C TAG Finding 22 January 2015," *W3C*. W3C, 2015.

[5] C. Morgan, "IAB Statement on Internet Confidentiality," *IAB*, 2014. [Online]. Available: https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality. [Accessed: 27-Nov-2018].

[6] T. Vyas and P. Dolanjski, "Communicating the Dangers of Non-Secure HTTP," *Mozilla Security Blog*, 2017. [Online]. Available: https://blog.mozilla.org/security/2017/01/20/communicating-the-dangers-of-non-secure-http. [Accessed: 27-Nov-2018].

[7] E. Schechter, "A secure web is here to stay," *Google Security Blog*, 2018. [Online]. Available: https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html. [Accessed: 27-Nov-2018].

[8] G. Ouvrier, M. Laterman, M. Arlitt, and N. Carlsson, "Characterizing the HTTPS Trust Landscape: A Passive View from the Edge," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 36–42, 2017.

[9] K. Bocek, "Is HTTPS enough to protect governments?," *Network Security*, vol. 2015, no. 9, pp. 5–8, 2015.

[10] European Commission, "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC," *European Commission*, 2017. [Online]. Available: http://ec.europa.eu/newsroom/dae/document.cfm?doc{_}id=41241.

[11] The European Parliament and the Council of The European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council," *Official Journal of the European Union*, no. 27 April 2. 2016.

[12] H. Gomes, A. Zúquete, G. P. Dias, and F. Marques, "Usage of HTTPS by Municipal Websites in Portugal," in *New Knowledge in Information Systems and Technologies. WorldCIST'19 2019. Advances in Intelligent Systems and Computing*, vol. 931, Á. Rocha, H. Adeli, L. Reis, and S. Costanzo, Eds. Springer, Cham, 2019, pp. 155–164.

[13] T. Berners-Lee, L. Masinter, and M. McCahill, "RFC 1738: Uniform Resource Locators (URL)," *IETF – Internet Engineering Task Force*, 1994. [Online]. Available: https://tools.ietf.org/html/rfc1738.

[14] P. Mockapetris, "RFC 1034: Domain Names – Concepts and Facilities," *IETF – Internet Engineering Task Force*, 1987. [Online]. Available: https://tools.ietf.org/html/rfc1034.

[15] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," *IETF – Internet Engineering Task Force*, 2008. [Online]. Available: https://tools.ietf.org/html/rfc5246.

[16] C. Jackson and A. Barth, "ForceHTTPS: Protecting High-Security Web Sites from Network Attacks," in *Proceeding of the 17th international conference on World Wide Web – WWW'08*, 2008, p. 525.

[17] J. Hodges, C. Jackson, and A. Barth, "RFC 6797: HTTP Strict Transport Security (HSTS)," *IETF – Internet Engineering Task Force*, 2012. [Online]. Available: https://tools.ietf.org/pdf/rfc6797.pdf.

[18] W. J. Buchanan, A. Woodward, and S. Helme, "Cryptography across industry sectors," *Journal of Cyber Security Technology*, vol. 1, no. 3–4, pp. 145–162, 2017.

[19] M. Kranch and J. Bonneau, "Upgrading HTTPS in mid-air: An Empirical Study of Strict Transport Security and Key Pinning," in *Proceedings 2015 Network and Distributed System Security Symposium*, 2015, pp. 8–11.

[20] S. Sivakorn, A. D. Keromytis, and J. Polakis, "That's the Way the Cookie Crumbles," in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society – WPES'16*, 2016, pp. 71–81.

[21] M. Ying and S. Q. Li, "CSP adoption: current status and future prospects," *Security and Communication Networks*, vol. 9, no. 17, pp. 4557–4573, Nov. 2016.

[22] A. Manousis, R. Ragsdale, B. Draffin, A. Agrawal, and V. Sekar, "Shedding Light on the Adoption of Let's Encrypt," *arXiv e-print arXiv:1611.00469*, Nov. 2016.

[23] T. van Goethem, P. Chen, N. Nikiforakis, L. Desmet, and W. Joosen, "Large-Scale Security Analysis of the Web: Challenges and Findings," in *Trust and Trustworthy Computing. Trust 2014. Lecture Notes in Computer Science*, vol. 8564, Springer, Cham, 2014, pp. 110–126.

[24] A. Andersdotter and A. Jensen-Urstad, "Evaluating Websites and Their Adherence to Data Protection Principles: Tools and Experiences," in *IFIP International Summer School on Privacy and Identity Management*, Springer, 2016, pp. 39–51.

[25] S. Englehardt and A. Narayanan, "Online tracking: A 1-million-site measurement and analysis," in *Proceedings of ACM CCS 2016*, 2016.

[26] P. Chen, L. Desmet, C. Huygens, and W. Joosen, "Longitudinal Study of the Use of Client-side Security Mechanisms on the European Web," in *Proceedings of the 25th International Conference Companion on World Wide Web – WWW'16 Companion*, 2016, no. September 2013, pp. 457–462.

[27] A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz, "Measuring HTTPS Adoption on the Web," in *26th Usenix Security Symposium*, 2017, pp. 1323–1338.

[28] A. P. Vumo, J. Spillner, and S. Kopsell, "Analysis of Mozambican websites: How do they protect their users?," in *2017 Information Security for South Africa (ISSA)*, 2017, pp. 90–97.

[29] M. Wullink, G. C. M. Moura, and C. Hesselman, "Dmap: Automating Domain Name Ecosystem Measurements and Applications," in *2018 Network Traffic Measurement and Analysis Conference (TMA)*, 2018, no. ii, pp. 1–8.

[30] C. Chan, R. Fontugne, K. Cho, and S. Goto, "Monitoring TLS adoption using backbone and edge traffic," in *IEEE INFOCOM 2018 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018, pp. 208–213.

[31] A. Lavrenovs and F. J. R. Melón, "HTTP security headers analysis of top one million websites," in *2018 10th International Conference on Cyber Conflict (CyCon)*, 2018, pp. 345–370.

[32] R. Robinson, "Urban vs. rural divide in HTTPS implementation for hospital websites in Illinois," *arXive eprint arXiv:1802.04159*, 2018.

[33] D. Kontogeorgis, K. Limniotis, and I. Kantzavelou, "An Evaluation of the HTTPS Adoption in Websites in Greece: Estimating the Users Awareness," in *Proceedings of the 22nd Pan-Hellenic Conference on Informatics – PCI'18*, 2018, pp. 46–51.

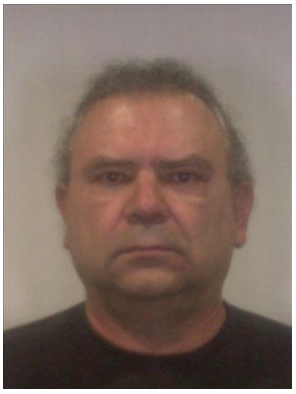
[34] L. Garron, A. B. Dropbox, and D. Boneh, "The State of HSTS Deployment: A Survey and Common Pitfalls," 2013. [Online]. Available: https://garron.net/crypto/hsts.

[35] G. P. Dias and M. Costa, "Significant socio-economic factors for local e-government development in Portugal," *Electronic Government, an International Journal*, vol. 10, no. 3–4, pp. 284–309, 2013.

[36] V. Pina, L. Torres, and S. Royo, "E-government evolution in EU local governments: A comparative perspective," *Online Information Review*, vol. 28, no. 4, pp. 1137–1168, 2009.

[37] Y. Chen, "Citizen-centric E-government services: Understanding integrated citizen service information systems," *Social Science Computer Review*, vol. 28, no. 4, pp. 427–442, 2010.
[38] G. P. Dias and H. Gomes, "Evolution of local e-government maturity in Portugal," in *9th Iberian Conference on Information Systems and Technologies (CISTI)*, 2014, pp. 1–5.

Biographies



Hélder Gomes holds a PhD in Computer Engineering from University of Aveiro (UA), Portugal, and currently he is adjunct professor at the School of Technology and Management of Águeda (ESTGA) and researcher at the Institute of Electronics and Informatics Engineering of Aveiro (IEETA) at UA. His main area of interest is computer security, with a focus on its application in the area of e-government and on user privacy, being the author of several scientific publications. Before joining the UA, he developed his professional activity as a Software Engineer having participated in several national and international projects on military tactical communications systems.

André Zúquete received his PhD in Informatics and Computer Engineering from Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal, in 2001. He is now Assistant Professor at University of Aveiro, Aveiro, Portugal, researcher of IEETA (Institute of Electronics and Informatics Engineering of Aveiro) and collaborator of IT (Instituto de Telecomunicações). His R&D activities are centered on the security in distributed systems, with a focus on the design of security architectures for several specific scenarios (e-Voting, e-Health, e-Government, vehicular networks, etc.). He is a program committee member of several conferences in the areas of security and mobility. He participated in several national and international projects and did some consulting on the security for Portuguese companies and state Departments. He has dozens of articles published in international forums related with security and mobility and he is the author of a technical book on network security (in Portuguese). He is the Portuguese representative on the IFIP TC11 (Security and Privacy Protection in Information Processing Systems).

Gonçalo Paiva Dias is associate professor at the School of Technology and Management of Águeda (ESTGA) and full researcher at the Research Unit

on Governance, Competitiveness and Public Policies (GOVCOPP) at the University of Aveiro. He held several positions at the University, including Vice Rector, Dean of ESTGA, and Director of the degree in Information Technology. He publishes regularly on the subjects of e-government, information systems and technologies, and higher education.

Fábio Marques completed his PhD in Computer Engineering (2013) at the University of Aveiro (UA). He is an adjunct professor at Escola Superior de Tecnologia e Gestão de Águeda (ESTGA-UA), where he teaches since 2001. He is a collaborator of the Institute of Electronic Engineering and Informatics of Aveiro (IEETA-UA). He is on the scientific committee of national and international journals and conferences. He has participated in several national and international projects, having also several publications. Currently, his research interests are in the areas of distributed systems, e-Government, Privacy and Educational Technologies.