Government Information Quarterly 31 (2014) S118–S125

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Web application vulnerability assessment and policy direction towards a secure smart government

Olusesan M. Awoleye [a,*], Blessing Ojuloge [b], Mathew O. Ilori [a]

[a] African Institute for Science Policy and Innovation (AISPI), Faculty of Technology, Obafemi Awolowo University, Ile-Ife, Nigeria
[b] National Centre for Technology Management, Agency of the Federal Ministry of Science & Technology, Obafemi Awolowo University, Ile-Ife, Nigeria

ARTICLE INFO

Available online 2 July 2014

Keywords:
E-government
Smart government
Web vulnerability
Policy
Cross site injection
SQL injection
Cookie manipulation

ABSTRACT

This paper carried out technological analysis of e-government platforms with a view of assessing possible application flaws that can inhibit smooth running of the available web services provided. Two sets of data were collected with an interval of two years on 64 Nigerian government websites. Five web vulnerability variables known to be notorious for web attacks were purposively investigated. In the overall assessment for the two datasets, the average result showed that about 67% are affected by broken links (BL), 43.8% by unencrypted password (UP), 35% by cross site scripting (XSS) and about one out of every four are affected by each of Structured Query Language Injection (SQLi) and cookie manipulation (CM). An independent t test statistic showed that there is a significant difference between the groups for three of the variables investigated, these are: XSS, SQLi and CM at 95% confidence interval. The motivation for this study is premised on the risk that these results pose to the smooth running of the e-government services and the possibility of financial loss. The research thus suggests some useful policy directions to enhance the provision of a secure smarter government.

1. Introduction

The growth of the internet and its services has brought innovation in the use of many web applications. This has provided sources of information for citizens and has created opportunities for businesses to thrive (Zhao & Zhao, 2010). Organizations and government bodies have leveraged severally on new technologies provided by the web for improved efficiency in service delivery, transparency, increased revenue, cost-saving and global competitiveness (Chen, 2002; Chen & Gant, 2001; Kim, Jeong, & Lee, 2009). Government services which have been characterized by rigid bureaucracy are gradually being taken over by e-government. When e-government services become more flexible to access for user's satisfaction it culminates into smarter government which is desirable (Rokhman, 2011). Smart government has been described as “the implementation of a set of business processes and underlying information technology capabilities that enable information to flow seamlessly across government agencies”. Smart government as an advanced government presents opportunities that people can avail themselves of, including: services, participation and communication anytime, anywhere and with any device through convergence and integration of smart IT and government services. It provides a platform where the government proactively pushes relevant, unique data to citizens based on their profiles. This helps government to provide real time information to her citizens. As changes occur to a citizen's circumstance, government processes are triggered to provide the appropriate service(s).

Despite the benefits of communication through the internet, the proliferation of cyber crime activities has created a big concern (Zhao & Zhao, 2010). For example in a world ranking survey of the top cyber crime perpetrators by country, Nigeria is rated 3rd behind United States and United Kingdom according to the Internet Crime Control Centre.[1] Since e-government projects are provided over an insecure channel like the internet, other important issues surface. In most countries (Nigeria inclusive), there are no governmental infrastructure that supports authentication, confidentiality, integrity and privacy issues (Moen, Klingsheim, Simonsen, & Hole, 2007). There are also other problems related to web applications that can give unexpected consequences when e-government solutions are deployed. It is worth noting to state that amid all these, the rate by which organizations and government are adopting the use of the web as useful resource is on the increase (Ebrahim & Irani, 2005; Gil-García & Martinez-Moyano, 2005; Wangpipatwong, Chutimaskul, & Papasratorn, 2005).

It has been identified that some of the motivations for adopting e-government have been largely technology pushed and benefit driven without given adequate attention to security issues. Quite a number of literatures have reiterated the consequence of porting ‘unverified’ web applications (Balduzzi, Gimenez, Balzarotti, & Kirda, 2010; Chien,

* Corresponding author at: African Institute for Science Policy and Innovation (AISPI), Faculty of Technology, Obafemi Awolowo University, Ile-Ife, Nigeria.
E-mail address: awoleye@yahoo.co.uk (O.M. Awoleye).

[1] www.ic3.gov/media/annualreport/2009_ic3report.pdf.

http://dx.doi.org/10.1016/j.giq.2014.01.012
0740-624X/© 2014 Elsevier Inc. All rights reserved.

2006; Moen, Klingsheim, Simonsen, & Hole, 2006, Zhao & Zhao, 2010). It is therefore expedient to investigate web related security threat(s) that may inhibit smooth running of e-government services. In this attempt, some useful research questions are raised viz: (i) what is the state of government websites relative to web vulnerability? (ii) Is there bias for category of organizations for the vulnerabilities? (iii) Is there any difference in the level of vulnerability of the websites over time? The following objectives are therefore drawn for this study: (i) to assess the level of vulnerability on government websites, (ii) to investigate vulnerability bias(es) for category of organizations, and (iii) to investigate the difference in web vulnerability over time. The rest of the study is organized as follows: the concept of evolutionary theory of change and e-government dynamics are discussed in Section 2. Section 3 discusses web application vulnerability while the methodology of the work is elucidated in Section 4. Section 5 present the findings of the two datasets collected. Section 6 discusses the summary and conclusion and presents some policy suggestions.

2. Evolutionary theory of technological change and e-government dynamics

This section discusses the theory adapted for this work, the evolutionary theory as posited by Nelson and Winter (1982). This is well placed since the process of e-government involves dynamic processes that require continuous development. The section also enumerates the dynamics of e-government; its overview and the situation in a few countries, especially Nigeria.

2.1. Evolutionary theory of technological change

The evolutionary theory of technological change as posited by Nelson and Winter (1982) and adapted by Metcalfe (1994) for technology policy and by Malerba, Nelson, Orsenigo, and Winter (1999) for the U.S. computer industry is well placed in our approach of smarter government which is evolutionary in nature. The process of evolution of e-government evolves from developing a web page to integrating government systems behind the web interface (Gil-García & Martinez-Moyano, 2005). Layne and Lee (2001) also described e-government as an evolutionary phenomenon which changes frequently with time. Some of the changes that have come over years have resulted in creating more complex websites beyond platforms that provides only information for the citizens. The process of creating more robust web platforms for additional services beyond informational services has culminated into an interactive and transactional system (Chan, Lau, & Pan, 2008). This system thus necessitates the creation of input fields on the websites such as web forms, logins, search, feedback. These efforts thus open the window of infiltration especially when the website is not properly checked for possible application errors (e.g. input validation).

2.2. E-government dynamics

Schelin (2003) described the evolvement of e-government from one stage to the other as necessitated by the quest for unhindered service. Each of these stages represents different levels of technological sophistication (Moon, 2002) towards improvement in quality of service delivery to the citizens. Describing the concept of e-government, we found diverse but related descriptions in literature. For example Backus (2001) defined e-government as the art of online administration of government activities. Whitson and Davis (2001) described it as a system that integrates cost-effective models for citizens, industries, federal employees, and other stakeholders to conduct business transactions online. Layne and Lee (2001) viewed e-government as government's use of technology, particularly web-based internet applications to enhance the access to and delivery of government information and service to citizens, business partners, employees, other agencies, and government entities. In the context of what this paper is set to address, Layne and Lee's (2001) description of e-government is accepted as our operational definition. E-government has the potential to help build better relationships between government and the public by making interaction with citizens smoother, easier, and more efficient. Indeed, the government can reach more citizens without boundary irrespective of their locations at any point in time. And in turn, the citizens can also reach the government without any bureaucracy barrier (Awoleye, Oluwaranti, Siyanbola, & Adagunodo, 2008).

To mention a few countries that have benefited from e-government activities, one will not hesitate to bring Korea into the picture. Korea is a good example that has used this service extensively and quite a lot of literatures about the approaches and the success of the Korean e-government project (Hee-joon, 2002a, 2002b; Sang-ho, 2002) are available. It was reported in the Korea e-Customs Service (KCS) that the trade volume of Korea increased by a multiple of 3.5. Also, duties and taxes collected as well grew by three times, while the number of KCS employees decreased by 6% (infoDev/World Bank, 2009). Taiwan has eased the difficulty of processing their income tax returns, which annually will process an average of over 4 million individual's tax returns manually (Wang, 2002). As reported by Wang (2002) during the tax-filing period, taxpayers perform complex calculations and fill out a standard printed form either by hand or typewriter. The tax return and related documentation are submitted to the tax agency over the counter or by postal mail. When using the manual filing method, taxpayers need to understand the individual income tax laws, and the tax return is subject to errors through writing and/or calculations. Internet filing was launched in Taiwan by the tax agency in 1998, which thus provide the taxpayers the platform to file their income tax returns via the internet and this eliminated the risk of computational errors which usually occurs when the tax is processed manually. Some other studies have shown positive rewards for e-government applications by different countries. For example, the one-stop shop portal (FirstGov) of the United States have aided many types of transactions ranging from Government to Consumer, Government to Business, and Government to Government and have been used for form downloads for most of public services and many more. Also in the United Kingdom, some of these services are in operation through the UK government online portal as presented by Anthopoulos, Siozos, and Soukalas (2007). Making services available online presents a better and easy way of government–citizen relationship, most especially on discharging obligations to the society. However, the concern now is the fear of adequate technical capability to handle possible susceptibility of the design of such platforms (websites), without which successful and smooth operation may be hampered.

2.3. E-governments in Nigeria

The emergence of e-government in Nigeria can be traced to the advent of democracy in 1999. Part of the responsibility of the National Information Technology Development Agency (NITDA) is to implement the Nigerian e-government initiative in conjunction with the National e-Government Strategy Limited (NeGSt) under a Public Private Partnership (PPP) model to guide the evolution of digital government solutions with consistent standards, operating platforms and applications across agencies and government systems in Nigeria (Fatile, 2012). More commitment has thereafter been shown by the federal government towards promoting ICT and e-culture through organizing several conferences and workshops to promote e-society awareness in the country (Ajayi, 2003; Ifenedo, 2006). These fora as reported by Ifenedo (2006) bring together local academia, businessmen, software multinationals and IT professionals and others from abroad. Some efforts by the government as well to facilitate the use of e-government have been identified. The government has created public awareness for e-government by providing Mobile Internet Units (MIU) for public use (Ifenedo, 2006). These are locally manufactured buses equipped with communication