Chapter 13
Security and Privacy Issues in E-Government

Ramaraj Palanisamy
St. Francis Xavier University, Canada

Bhasker Mukerji
St. Francis Xavier University, Canada

ABSTRACT

Government is a unique actor as a provider of online public services to its citizens and enterprises. The e-citizens expect that the e-government services are safe and secure, that the privacy of the e-citizen is protected. As security and privacy are primary concerns in e-government, this chapter describes the security and privacy issues faced by the government, the sources and applications of these threats, the ways of protecting security and citizens' personal information, and the challenges in managing the security threats. The purpose of this chapter is to provide guidelines for the administrators of state-level & federal-level e-government services and IT professionals that they need for continuous improvement of e-government security and privacy.

INTRODUCTION

As web technologies have developed from the pure information-sharing phase to interactive, transactional, and intelligent phases, many states and countries started making use of these technologies for web-based government (e-government) services for improving government efficiency, transparency, and competitiveness in the global economy. Over 90% of United Nations member countries now operate their government Websites (Swartz, 2004) and engage their e-citizens in e-government systems and services. The businesses and citizens easily find the information or services they need by using the e-government websites and thereby strengthening their competitiveness and growth (Brush, 2007). The easy access to the e-government websites for availing the government services has made the government more transparent and efficient (Digital Task Force, 2004). The

DOI: 10.4018/978-1-60960-848-4.ch013

e-government benefits are numerous: U.S. federal e-government saved more than U.S. $133 million in software costs (Evans, 2008); about four million citizens filed income taxes online for free in 2007 by using IRS Free File; Forrester Research predicts that more than $600 billion of government fees and taxes will be processed Worldwide through the web; in Europe citizens saved seven million hours a year on the time they spent for filing income taxes; European Union firms save about € 10 per transaction when doing it online (European Commission, 2005) to name a few. Chevallerau (2005) identified several tangible benefits of e-government: improved quality of information supply, reduced work-process time, fewer administrative burdens, reduced operational cost, improved service level, increased work efficiency, and increased customer satisfaction.

Despite the increasing popularity and substantial growth in the development of e-government services on the internet, the e-government stumbles upon security and privacy threats (Thibodeau, 2000). In general, the internet users have growing concerns of cyberspace identity thefts and privacy violations. Citizens may be skeptical and mistrust e-government services, perceiving them as invasions of citizens' security and privacy (James, 2000). Security and privacy issues are big concerns in using commercial Websites; there is even more of a concern for citizens engaging with e-government services (McDowell, 2002), led to a lack of trust which was identified to be a significant barrier to the adoption of e-government (Cremonini and Valeri, 2003). The e-government sites become potential targets for cyber attackers and terrorists. Cyber intrusions into e-government network systems could harm e-government services any time if the e-government sites were not properly secured (Halcnin, 2004). Moen et al., (2007) reported that 82% of the e-government sites around the world were vulnerable to common web application attacks such as cross site scripting and structured query language (SQL) injection. In particular, 90% of the European e-government sites and 76% of the North American (United States and Canada) e-government sites were vulnerable to common web application attacks. The U.S. was targeted by most denial of services (DoS) attacks during the first half of 2007, accounting for 61% of the worldwide total (Symantec, 2007). The types of cyber intrusions and attacks were DoS attacks, unauthorized access to networks, theft of employee or customer information, online financial fraud, website defacement, web-application attacks, and system penetration (e.g., Halcnin, 2004; Moen et al., 2007; Richardson, 2008; Symantec, 2007). These attacks mainly aimed networks` TCP/IP (Layer 4), SSL (Layer 5), HTTP and FTP (Layer 7) according to the Open Systems Interconnection Reference Model (McNurlin & Sprague, 2006). Besides, some states and local e-government sites posted citizens` names, social security numbers, property tax records, or other private information on their site without any password protection (Myers, 2007). This private information lured the cyber attackers for causing nuisance, destructive attacks, and misusing this for financial gains (Symantec, 2007).

Government is a unique actor as a supplier of online public services to its citizens and enterprises, arguably, it is of primary importance that the usage of e-government services is safe and secure, that the privacy of the e-citizens is protected. As security concerns are an important reason for people not to access the Internet, this chapter describes the security and privacy issues faced by the e-government, the sources and applications of these threats, the ways of protecting security as well as citizens` personal information, and the challenges in managing the security threats. The purpose of this chapter is to provide guidelines for the administrators of state-level & federal-level e-government services and IT professionals that they need for continuous improvement of e-government security and privacy.