

An Analysis of Identity Theft Safeguards in the U.S. e-Government Systems

Jungwoo Ryoo*
Penn State Univ.
jryoo@psu.edu

Tae H. Oh
Southern Methodist Univ.
taehwan@engr.smu.edu

Seungjae Shin
James Madison Univ.
sshin@meridian.msstate.edu

Young B. Choi
Mississippi State Univ.
choiyb@jmu.edu

1 Introduction

Today, the use of Information and Communication Technology (ICT) is transforming the ways many organizations conduct their business. Governments are no exception from this phenomenon, and their use of ICT in providing services (to the public or other government organizations) is referred to as Electronic Government (e-Government). More specifically, Gartner Group defined e-Government as “the continuous optimization of service delivery, constituency participation, governance by transforming internal and external relationships through technology, the Internet, and new media [14].

Under the banner of e-Government, more and more governmental organizations are making information available online. Not every piece of information served by e-Government Web sites are susceptible to harassment, but some do have a potential for attracting criminals who are constantly looking for opportunities to abuse these public resources. For instance, many e-Government sites handle sensitive personal information such as Social Security Number (SSN), driver’s license information, medical history, birth certificate details, etc. Once stolen, this information can be used for various criminal activities ranging from identity theft to terrorist attacks. By providing e-Government contents on mobile wireless devices, the recent trend toward mobile government (m-Government) [12] even further exacerbates the security risk.

There are two major elements in e-Government security on the Internet: the client and server-side systems. The server-side systems refer to an information systems infrastructure allowing one to store and manipulate data and is implemented by hardware and software. The client-side system provides interfaces through which end users interact with the server-side system. Security vulnerabilities could exist in both client and server-side systems. In this paper, we concentrate on the client part (especially, Web interfaces) of e-Government security and attempt to investigate the security practices (particularly concerning identity theft) of a carefully selected set of heavily used e-Government Web sites in the U.S.

More specifically, the Research Objectives (ROs) of this paper are:

- **RO 1:** Exploring the types of information available on the e-Government sites and creating a taxonomy,

*Corresponding author

- **RO 2:** Identifying the dimensions of the taxonomy of developed in RO 1, which demands identity theft-related security protection,
- **RO 3:** Analyzing the identity theft-related security safeguards currently employed by e-Government sites and reporting the results,
- **RO 4:** Comparing the findings from RO 3 with the best practices and finding deficiencies if there is any, and
- **RO 5:** Identifying e-Government-specific security requirements regarding identity theft and providing suggestions for how to address those needs.

We examine e-Government sites respectively for local, state, and federal governments in the U.S.

The findings of this study will not only help these different types of e-Governments improve the security of their Web sites but also aid policy makers in understanding the potential loopholes that could lead to future security breaches and develop appropriate policies to regulate the implementation of e-Governments in the Cyberspace.

2 Taxonomy of E-government Information Resources

There are two major aspects to take into account when considering possible e-government information resources. The first (referred to as *offered data* in this paper) is obviously the information available through the various services offered by the e-government Web sites. This type of data is typically collected through conventional means such as filling out paperwork, etc. The second (referred to as *acquired data*) is the information requested (either explicitly or implicitly) and collected by the e-government sites as a precondition to providing the offered data. These pieces of data include e-mail addresses, user name, passwords, credit card numbers, cookies, Internet Protocol (IP) addresses, Operating System (OS) types, etc. Therefore, the taxonomy we are proposing has offered and acquired data as its top level categories.

The acquired data category is then further categorized by how the requested data is obtained. If the data request is explicitly conveyed to a user, we call the returned data *explicitly acquired data*. Many e-government sites allow users to register themselves for easier subsequent accesses, and they in return require their users to provide information uniquely identifying them. User names, passwords, mother's maiden name, etc. In this case, the data collected is mainly used for access control purposes. Other purposes for the explicitly acquired data include payment-related data like credit card information, contact data (e-mail addresses, phone numbers, home addresses, etc.), and quality control data that could be elicited through survey questions. From the discussion above, it is now self-evident that one can use the purposes of data collection to further categorize the explicitly acquired data category of our taxonomy.

A counterpart category of the explicitly acquired data is the *implicitly acquired data* that are gathered without a direct consent from the person whose personal data is extracted from a transaction between the person's Web browser and the Web server hosting the e-government site. Once again, the implicitly acquired data can be classified into sub-categories by the purposes of data collection including surveillance, demographic, and automation. Surveillance data refers to the networking information (for example, IP addresses, type of an operating system or Web browsers used by the end user) collected for monitoring purposes. Demographic data is sought for understanding the

demographic characteristics of the e-government service consumers and could be derived from the surveillance data. For example, through IP route tracing, it is possible to know which geographical region an end user is from. Finally, the automation data is used to promote convenience and efficiency of both customers and e-government site maintainers. For instance, cookies are text files widely used for a Web browser to store a user name and feed it directly to the browser without a user intervention so that the users do not have to enter it every time he or she logs on to an e-government site.

We make the sub-categories of the offered data category of our taxonomy surface by applying the target audience type of e-government services as a criterion. Target audience here means persons from whom the e-government services are intended. There are largely three target audience types: individuals, businesses, and other government organizations. Therefore, there are also three corresponding data types available to these target audience types: *individual service data*, *business service data*, and *government service data*. The individual service data is available when a branch of the government establishes a direct relationship with citizens individually. The sub-categories of the individual service data include: tax (income taxes, property taxes, etc.), job postings, social security (unemployment benefits, student grants, medicare, etc.), personal documents (driver's license and passports), registrations (cars), applications (building), declaration (theft), reporting (change of address) certificates (birth and marriage), public libraries, and health data.

The business service data is available for the business organization that are in a relationship with the government either in a citizen-like role or as a service provider. When playing the citizen-like role, a businesses acts as a citizen by providing or consuming data similar to those described in the individual service data description. After all, businesses pay taxes and rely on many services offered by the government. The government service data is exchanged between government organizations providing services to each other. Since the focus of this paper is on the identity theft problem of individual citizens, the sub-categories of the business and government service data categories are not relevant to our taxonomy, and we do not elaborate their details.

3 Identity Theft Relevant E-Government Data Resources

Among the data resources categories introduced in the previous section, some are particularly vulnerable to identity theft attempts while others are completely irrelevant. In this section, we present a set of criteria for checking the relevance of each data category for their relevance to identity theft and identify all the identity theft relevant categories out of our e-government data resources taxonomy.

3.1 Identity Theft Relevance Criteria

If a data source meets at least one of the criteria explained below, we identify it as an identity theft-relevant e-government data resource.

3.1.1 Aid to Establish a Digital Identity on the Same E-Government Site (AEDIS)

This criteria is used to evaluate whether a data resource category is a significant aid to an identity thief in establishing a digital identity on the same e-government site he or she is compromising.

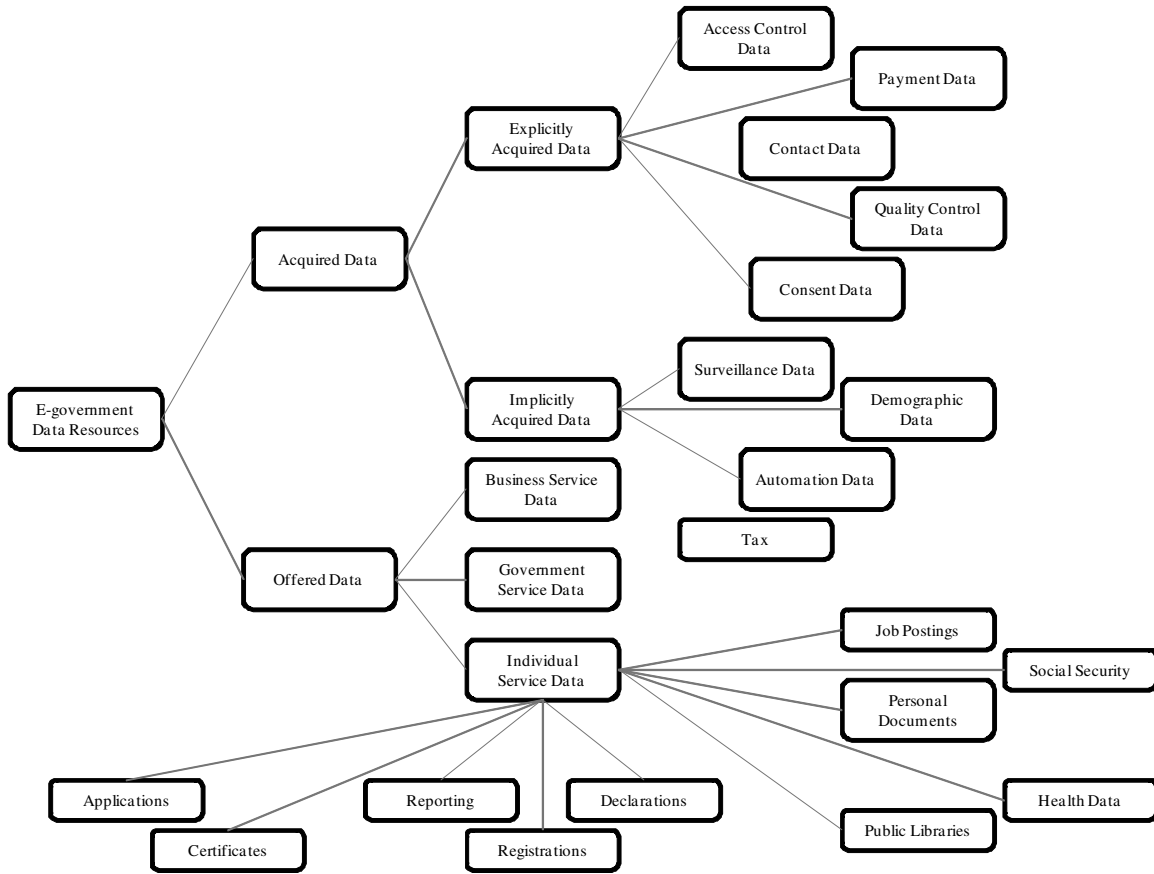


Figure 1: The Proposed Taxonomy of E-Government Data Resources

In most cases, simply stealing a user names and its corresponding password is enough. The data resources category meeting this criterion typically help guess the user names and passwords. First names, last names, e-mail addresses, and phone numbers are good examples of this type of data resources.

3.1.2 Aid to Establish a Digital Identity in the Cyberspace in General (AEDIC)

People often have multiple Web accounts. Stolen information (one or more of the e-government data resources) from an e-government site can therefore be used to establish an identity that are tied to multiple Web accounts. When using the same user name and password for many different online accounts, a person can fall an easy prey to a scheme that rely on the data sources conforming to this criterion. For example, one may use the same user name and password for his or her e-government site and online banking system. Once knowing the details of the e-government account, an identity thief can take over the person’s entire financial identity.

3.1.3 Aid to Establish a Real-World Identity (AERWI)

In the best case scenario, an identity thief can ascertain enough information to construct a person’s real-world identity from various e-government data resources. In fact, stealing one’s digital identity

(whether for a single or multiple sites or not) can greatly accelerate an identity thief’s effort to collect sufficient information to accomplish the task of stealing one’s real-world identity. As a result, the data resources satisfying the above two criteria certainly meet this criterion. When having access to one’s birth certificate, driver’s license, or tax return, an identity thief’s job to steal the person’s real-life identity becomes much easier.

3.2 Classification Results

Figure 2 shows the results of our classification results for the identity theft-relevant e-government data resources. The identity theft-relevant data resources are marked by ×.

			AEDIS	AEDIC	AERWI	
E-Government Data Resources	Acquired Data	Explicitly Acquired Data	Access Control Data	X	X	X
			Payment Data	X	X	X
			Contact Data	X	X	X
			Quality Control Data			
			Consent Data			
		Implicitly Acquired Data	Surveillance Data			
			Demographic Data	X	X	X
	Automation Data		X	X	X	
	Offered Data	Business Service Data	N/A			
		Government Service Data	N/A			
		Individual Service Data	Tax	X	X	X
			Job Postings			
			Social Security	X	X	X
			Personal Documents	X	X	X
			Health Data	X	X	X
			Public Libraries			
			Application	X	X	X
			Certification	X	X	X
			Reporting	X	X	X
Registration			X	X	X	
Declaration	X	X	X			

Figure 2: Relevance Classification of the E-Government Information Resources

4 Identity Theft Attack Methods

Identity theft attacks against e-government Web sites can be mounted in many ways. In this section, we will look into each of these methods to facilitate our later discussions on preventive measures and a new assessment framework we developed for this paper.

4.1 Pure Social Engineering

Social engineering refers to a psychological attack taking advantage of human vulnerability in falling for disingenuous schemes to obtain confidential personal information. Social engineering is typically used in conjunction with computer and networking technologies such as e-mails (as in phishing

explained in the next section). By *pure* social engineering we mean that no such technologies are involved in the attack.

In the context of e-government, someone might pose as a government official on the phone and try to threaten people reveal online account or other information to establish a digital identity elsewhere for malicious purposes.

4.2 Phishing

Phishing is one of the most common identity theft techniques in use today. Through various means (discussed in the ensuing subsections), citizens are led to a fraudulent Web site where they are prompted with an online form requesting sensitive personal information such as Social Security Number (SSN), credit card number, etc. Identity thieves lure their victims into a fake site by one of the methods described below.

4.2.1 Electronic Mails

Attackers send seemingly authentic electronic mails with embedded links to the malicious site.

4.2.2 Local Hosts File

The hosts file (locally stored on a computer) holds mappings between Internet Protocol (IP) addresses (numeric addresses meant for machine consumption) and host names (meaningful names meant for human use). Attackers can compromise the computer and install malicious software to change the content of the local host file so that users are directed to a rogue Web site although providing a correct host name (or URL).

4.2.3 DNS Server

A Domain Name Service (DNS) server is a service running on a remote computer and translates host names into IP addresses. Attackers can also compromise the DNS server and change the mapping between the host names and IP addresses.

4.2.4 Proxy Server

A proxy server resides between a client machine and a remote Web server, and caches Internet contents so that a Web browser on the client machine does not have to retrieve the same information repeatedly from the Web server, which in turn helps performance.

Attackers can take over a proxy server, intercept a request for a legitimate Web site, and redirect it to an illegitimate Web site of their interest without the knowledge of the user.

4.2.5 Man-in-the-Middle Attack

This attack is similar with the proxy server attack described above in a sense that a malicious third party is intercepting network traffic between two innocent victims communicating with each other.

The difference is that this attack does not involve compromising a proxy server, and attackers can freely steal information from the existing communication channel. They can also embed their own content into a Web page presented to a user to mislead them.

4.3 Password Cracking

There are primarily two types of password cracking attacks: brute force and dictionary attacks. Attackers attempt to gain access to an e-government Web site by trying arbitrary user name and password combinations in the brute force attack scenario while words appearing in the dictionary are first tried in the dictionary password attacks.

5 Evaluation Framework

In this section, we examine well-known ‘best practices’ in thwarting identity thieves, which are relevant to e-government settings. Many of the best practices come from the e-commerce literature since e-government could also be viewed as another form of e-commerce systems although the services provided are not for profit. The best practices are presented in terms of safeguards, each of which will eventually be used as one of the criteria to evaluate e-government Web sites based on its adoption. If necessary, we will also study the level of adoption since how a best practice safeguard is implemented makes a big difference in the success of a protection attempt.

Safeguards against identity theft can be considered in the following three major categories:

- **Security control** refers to a set of *technical* countermeasures designed and implemented to discourage, prevent identity theft attempts, or minimize the damage when an identity theft actually occurs.
- **Privacy control** relies on the security control, but it involves much more than just technologies and means a conscious decision (by those collecting personal information) regarding the limitation imposed upon the use of the collected sensitive information. A prime example for an organization’s decision on privacy is a policy on whether to sell customer information to the third party or not.
- **Awareness control** is efforts made by a service provider to promote the degree of understanding among users on the dangers of identity theft, precautions people can take to proactively avoid falling a prey to identity thieves, how to respond to an identity theft incident, and how to report suspicious activities, etc.

Although the focus of our paper is mainly on the security protections, we do look into all the major mechanisms involved in privacy protections and awareness promotion methods.

Most of the identity theft attack methods discussed in section 4 are preventable by deploying one or more of the controls introduced in this section. For example, pure social engineering attacks can be effectively neutralized by strong strong awareness control while phishing and password cracking attacks can be significantly curbed by employing better security and privacy controls.

5.1 Security Control

Access control, cryptography, and digital identity hardening are three major security control implementation types available for e-government Web sites. In this section, we will describe all the mainstream examples of these three security control approaches.

5.1.1 Access Control Methods

Access control can be sub-divided into:

- identification: “the means by which a user provides a claim of his or her identity to a system” [15],
- authentication: verification of the claimed identity of a person,
- authorization: assignments of access rights to computing resources, and
- auditing: supervision of the activities of an authorized user in a certain computing environment.

Most of the access control mechanisms used in an e-government environment adopt at least identification and authentication controls. Some do implement authorization and auditing, but we do not discuss them here since their presence is difficult to verify from the client side.

- Passwords: Passwords are the most common form of access control method found on e-government Web sites. There are mainly two types of passwords:
 - **Conventional Passwords** refer to a secret combination of numbers, regular characters, and special characters that is provided to a protected system to gain access.
 - **One-time Passwords** are different from conventional password in that they are generated by a machine instead of a human user and used only once as their name suggests. There are also two primary types of one-time passwords:
 - * **Software Token Devices** are typically built into a computer system and used together with conventional passwords. Once users are logged onto the system using the conventional password, he or she is implicitly issued with a one time password. The password then allows the user to have access to other resources within a computing environment without having to authenticate himself or herself repeatedly. Software token device-based passwords are also called tickets, and the systems implementing the software token mechanism are called *single sign-on* systems.
 - * **Hardware Token Devices** are packaged into a portable, physical device that can be easily carried by a user. As in the software token devices, these devices first require users to log in using their conventional passwords and to enter a string the hardware token devices display.
 - * **Use of Clipping Levels:** clipping levels refer to a threshold allowed for mistakes made by users when entering their passwords. Systems implementing clipping levels lock users out for a certain period of time or until a new password is issued when a predefined clipping level limit is reached.

- **Passphrase:** Passphrases are almost like passwords except for the fact that they can contain spaces and consist of a longer string.
- **Federated Identity:** Federated identity is a distributed user authentication technology that allows users to log on to the Web sites of disparate organizations in different business domains [21]. In an e-government scenario, federated identity can be used to enable users to use their identity credentials over many different government Web sites such as federal, state, and local governments. Trust is the key to the successful implementation of federated identity since user credentials provided to one provider is shared among multiple ones trusting each other in a federated identity system.
- **Anti-phishing Measures:** There are several anti-phishing measures e-government Web sites can adopt [11]:
 - **Use of Personalized Information:** User chooses an image or text when they create their account. The image or text is presented to users in the subsequent log-in attempts to verify the authenticity of the provider.
 - **Interfering with Navigation:** A warning message can be displayed to ensure that users are aware of the danger of jumping from one Web site to another using an embedded link on a Web site.
 - **Detecting Inconsistent DNS Information:** E-government Web sites can keep track of DNS look-up results and warning messages can be presented to users if a DNS resolution result is different from the one kept from earlier transactions.
 - **Cross-site Scripting Filtering:** E-government Web sites can be designed to filter a certain portion of user-supplied data to prevent cross-site scripting filtering.
 - **Password Hashing:** This ensures that no password information is sent to a Web server as part of a plain text URL. The password information is hashed and then combined with the URL information.
- **Centralized registration:** Under this scheme, users register themselves once at a central Web location made available by a branch of government. The user credentials are shared among multiple sites supported by the same authentication service such as a shared Lightweight Directory Access Protocol (LDAP) database. LDAP is a common directory server implementation widely used by organizations to manage information on individuals, such as name, phone number, etc. The use of centralized registration reduces the probability of sensitive personal information to be stolen since the approach minimizes the possibility of keeping multiple copies of private user data across many different systems.

One way to implement centralized registration is a state or inter-agency federal effort to create a Web infrastructure to help local governments, other state government organizations, and other federal agencies in collecting and managing user information for access control in addition to building their own e-government sites.

For instance, many state governments have an independent arm that specializes in building and maintaining Information Technology (IT) infrastructures including maintaining a central Web site for logging in and providing Web hosting services at discount pricing.

The obvious downside of this approach is the problem of single point of failure. That is, once the centralized registration site crashes, all the sites using the service is not accessible, therefore negatively affecting the availability aspect of security. However, this practice, in

general, can be regarded as a better security measure against identity theft than allowing multiple independent sites collecting and maintaining sensitive personal information.

5.1.2 Cryptography

Cryptography is another generic term referring to a set of security technologies that turn a plain text string into a cipher text counterpart to ensure confidentiality of data being transferred. There are two most common cryptography technologies in use today in the e-government settings:

- **Public Key Infrastructure (PKI):** PKI ensures message confidentiality, message integrity, and user authentication without letting two communicating parties exchange any secret information before the start of their communication. This is accomplished by the use of a third party (called CA or Certificate Authority) that verifies the authenticity of the two communicating parties. The use of PKI has been promoted by the federal government for many of its Web applications. One of the challenges faced by e-governments when implementing PKI is the existence of multiple CAs using different technologies among various government organizations [1]. The interoperability problem must be resolved first before the widespread use of PKI in the e-government domain.
- **Secure Socket Layer (SSL):** This technology allows data entered through a Web client to be encrypted before being sent to its destination. For example, credit card information is sent using the SSL technology over the Internet to prevent hackers from stealing the information. Most of Web browsers show a small lock sign when SSL is being used.

5.1.3 Digital Identity Hardening

Digital identity hardening means requiring extra rigor when a user is trying to establish his or her digital identity for an e-government system. Two separate steps can be taken for hardening a digital identity [3]. Validating is the first step that ensures the existence of a claimed identity (as in identification of access control). Verification is next step that authenticates a person's claim for his or her association with a specific identity. In countries such as United Kingdom (UK) or Korea, citizens are asked to show up in person and provide multiple documents to prove their identity before they are given a digital identity along with extra security measures such as a digital certificate.

5.2 Privacy Control

5.2.1 Use of Minimum Information

To protect the privacy of individuals, many e-government sites strive to minimize the amount of information being collected from their Web sites in return for services they provide. Federal Web sites recently stopped using cookies to promote this minimum information collection principle. In many cases, the e-government Web sites try to let their users be aware of their effort to collect only necessary information to address the privacy concerns.

5.3 Awareness Control

5.3.1 Security Certifications and Seals

To alleviate user concerns on security breaches resulting from e-commerce transactions, many commercial Web sites now apply for security certification that is provided by a trust third party. The security certification companies not only help identify potential security holes on a Web site but also offer seals that could be shown on a Web page intended to boost the credibility of the service provider in terms of its security readiness. Although many companies in the private sector offer security certification services, there is currently no government oversight (such as standards or regulations) that ensures the quality of services provided by these companies. Some of the well known security certification services include TRUSTe, BBBOnline, and WebTrust.

5.3.2 Use of Security Statements

Although an e-government Web site employees all the necessary security safeguards discussed in the security section, potential users will still be reluctant to use the services available on the Web site unless the site has a page that explicitly explains what kinds of precautions have been taken to protect transactions occurring on the site. Therefore, it is critical to have well written security statements to promote the use of an e-government Web site.

5.3.3 Use of Privacy Statements

The privacy provisions of the e-Government Act of 2002 demands both a “human readable” privacy policy and use of machine readable technology that automatically processes privacy policy statements and warns users for discrepancies between the privacy policy and a predefined set of user privacy preferences. Therefore, the use of privacy statements is an important barometer that shows whether an e-government Web site is practicing proper privacy controls or not.

5.3.4 The Platform for Privacy Preferences (P3P)

Most of users do not care to read privacy statements provided by an e-government Web site. This is often the case because the privacy statements tend to be lengthy, too dry, and difficult to navigate. The P3P technology has been developed to make it easier and less painful for users to check the relevant contents of a privacy statement by automating part of the privacy statement delivery mechanism. To accomplish this goal, users are asked to configure a P3P system to look for certain privacy-related terms and conditions. A P3P-enabled Web page will therefore interact with the P3P client installed on the user’s computer and alert him or her if there is any privacy statement of the user’s interest.

6 Assessment of e-Government Sites

This section discusses the results of evaluating e-government Web sites for their (identity theft-specific) security readiness using the evaluation criteria we developed in the previous section.

6.1 Selection Criteria

Due to the personal nature of identity theft crimes, the e-government Web sites we selected for evaluation had to be those directly interacting with individuals. In addition, the Web sites had to contain relevant data resources (AEDIS, AEDIC, and AERWI discussed in section 3.1) for identity theft. Most of the state and local government Web sites satisfied these criteria, and we therefore used the top ten e-government Web sites rated by the Computer World magazine [5] for our evaluation. Federal e-government Web sites were more difficult to choose since many of them serve other government agencies instead of individuals and did not have data resources for this research.

6.2 Federal Governments

Since U.S. Congress passed the Federal Information Security Management Act of 2002 (FISMA), GAO (Government Accountability Office), an agency for U.S. Congress, has investigated 24 federal agencies' information systems and evaluated the adequacy and effectiveness of the agencies' information security policies and practices as well as their implementation of FISMA requirements. The report of 2007 [13] states that many agencies have placed sensitive data at risk, which could lead to loss of privacy and potential identify theft. In the report, the GAO categorizes information security weaknesses into five areas (i.e., access control, configuration management, segregation of duties, continuity of operation, and information security program). Among them, access control matches one of the identity theft readiness evaluation criteria we described in the previous section. 22 out of 24 agencies had access control weaknesses, and in all security weaknesses identified by the GAO, 74% were access control weaknesses [13].

In the privacy control, there were many incidents reported by the federal agencies in 2006. Some of the agencies lost computer equipment such as laptops, USB drives, hard drives containing personally identifiable information like name, social security number, etc. Some agencies accidentally posted personal information on their web site or released CDs containing personal information. Other agencies experienced a security breach of their firewalls and compromises in computer communications systems for e-mail and instant messaging. The following table summarizes examples of security incidents in the privacy control category which GAO found in its report [13].

For the awareness category of our evaluation, we investigated 24 federal agencies' Web sites to check whether they have explicit statements of privacy and security policies. Among the 24 federal agencies' web sites, most of them have a 'privacy notice' menu in the top or bottom of their initial web page, which users can easily access. In their privacy notice web pages, they give statements such as why they collect users' personal information, how they will use users' personal information, who they will share users' personal information with, and/or how to use cookies in their web sites. For the security notice, most of them put it as a subsection of privacy notice. The security section often states that the agency will use a special program for monitoring network traffic to identify unauthorized attempts to cause damage to their information systems. But none of the agencies' security notices say how to avoid identity theft, how dangerous it is, and/or how to report suspicious activities.

				http://www.michigan.gov/	http://www.accessidaho.org/	http://www.in.gov/	http://www.nebraska.gov/	http://www.utah.gov/	http://az.gov/	http://www.state.ar.us/	http://www.colorado.gov/	http://www.georgia.gov/	http://www.state.tx.us/	
Security Control	Passwords	Conventional		X	X	X	X	X	X	X	X	X	X	
		One-time	Software Token											
			Hardware Token											
	Passphrase													
	Federated Identity													
	Anti-phishing Measures	Personalized Information												
		Navigation Interference		X	X	X	X	X	X	X	X	X	X	X
		Inconsistent DNS Detection												
		Cross-site Scripting Filtering		X	X	X	X							
	Password Hashing		X	X	X	X			X	X	X	X		
	Centralized Registration		X	X	X	X			X	X	X	X		
Cryptography	Public Key Infrastructure (PKI)													
	Secure Socket Layer (SSL)		X	X	X	X	X	X	X	X	X	X	X	
Privacy Control	Use of Minimum Information		X	X	X	X	X	X	X	X	X	X	X	
Awareness Control	Security Certifications and Seals													
	Use of Security Statements													
	Use of Privacy Statements		X	X	X	X	X	X	X	X	X	X	X	
	The Platform for Privacy Preferences (P3P)													

Figure 3: Assessment Results for State E-government Web Sites

6.3 State Governments

Table 3 summarizes the identity theft readiness assessment results for the state e-government Web sites. The leftmost column of the table shows the three major evaluation criteria (i.e., security, privacy, and awareness controls) we used for the evaluation. Each of these major evaluation criteria has its own sub-categories that can also be further divided depending on the need. An X mark is used to denote that an e-government Web site implements a certain anti-identity theft safeguard for a given evaluation criterion. For example, the Michigan state government Web site allows users to register themselves on the Web site and provide an ability to use a user name and password combination, which is why the categories like conventional password and centralized registration are marked in the table. At the same time, this use of conventional passwords and centralized registration disqualifies the Web site for the minimum use of information since a lot of unnecessary information for providing online services is collected when users registers themselves. For payments made online, the site also uses SSL to encrypt sensitive financial information provided by a user and then sends it to a server. Security and Privacy policy rows are also marked since the Web site does post these policies. The site does not provide any anti-phishing measures described earlier.

7 Conclusion

One of the most important contributions of this paper is the creation of a novel data resources taxonomy that identifies e-government-centric data types relevant to identity theft readiness assessment. In addition, an assessment framework consisting of a comprehensive set of identity theft readiness testing criteria has been developed. By using real federal, state, and local e-government Web sites, We demonstrated that one can systematically evaluate an e-government site for their identity theft readiness. Since the focus of the paper has not been an extensive assessment of the U.S. e-government Web sites, the evaluation section of this paper is exploratory in nature. Therefore, the limited evaluation we provide in this paper only provides snapshots of the status quo of the readiness in some of the most popular e-government Web sites in the U.S. Once the data resources taxonomy and the evaluation framework are mature and stable enough, we plan to conduct a full scale assessment study.

References

- [1] Peter Alterman. The us federal pki and the federal bridge certification authority. *Computer Networks*, 37(6):685–690, December 2001.
- [2] Király András. Credential-based implementations of digital identity for non-traceable access to e-government services. Master’s thesis, University of Zürich, 2003.
- [3] Stephen Mason Barrister. Validating identity for the electronic environment. *Computer Law and Security Report*, 20(3):164–170, may 2004.
- [4] France Belanger and Jannie S. Hiller. A framework for e-government: Privacy implications. *Business Process Management Journal*, 12(1):48–60, 2006.
- [5] Mitch Betts. Report card: the best e-government sites: A study of the best state and local government web sites, 2007. <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005371>.
- [6] Paul Beynon-Davies. Personal identity management and electronic government-the case of the national identity card in the uk. *Journal of Enterprise Information Management*, 20(3):244–270, 2007.
- [7] Michael Caloyannides, Dennis R. Copeland, George H. Datesman Jr., and David S. Weitzel. Us e-government authentication framework and programs. *IT Professional*, 5(3):16–21, May/June 2003.
- [8] L. J. Camp. Identity, authentication, and identifiers in digital government. In *Proceedings of 2003 International Symposium on Technology and Society-Crime Prevention, Security, and Design (ISTAS/CPTED 2003)*, pages 10–13, 2003.
- [9] L. Jean Camp. Identity in digital government, 2003. <http://www.lsi.upc.edu/~jvazquez/docs/EULAT-biometrics.PDF>.
- [10] Sebastian Clauß and Marit Köhntop. Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219, October 2001.

- [11] Aaron Emigh. Online identity theft: Phishing technology, chokepoints, and countermeasures. Technical report, United States Department of Homeland Security, October 2005.
- [12] A. Ghyasi and I. Kushchu. Uses of mobile government in developing countries. <http://www.mgovlab.org>, 2004.
- [13] Government Accountability Office. Information security. Technical Report GAO-07-837, United States Government Accountability Office (GAO), 2007.
- [14] Gartner Group. Key issues in e-government strategy and management. Research Notes, Key Issues, 2000.
- [15] Shon Harris. *CISSP Certification*. McGraw Hill, second edition, 2003.
- [16] Amir Hayat and Thomas Rössler. Proposed framework for an interoperable electronic identity management system. In *Proceedings of International Conference on e-Government*, 2006.
- [17] Noorliza Karia and Muhammad Hasmi Abu Hassan Asaari. Identity theft: What can be learned? In *Proceedings of 2nd International Conference on Disaster Management Preparing for the Future*, 2001.
- [18] Nico Maibaum, Igor Sedov, and Clemens H. Cap. A citizen digital assistant for e-government. *Lecture Notes in Computer Science*, 2456/2002:139–175, February 2002.
- [19] Jeffrey Roy. National identity and confidential interoperability: Does canada need a new identity card? *Policy Options*, pages 24–29, July-August 2006.
- [20] Milind Sathye, Eugene Clark, and Anni Dugdale. Fraud in e-government transactions: Risks and remedies. Technical report, Australian Government Information Management Office, Department of Finance and Administration, 2004. http://www.agimo.gov.au/publications/2004/05/egovt_challenges/privacy/fraud.
- [21] Francis Vierboom. Distributed identity part 2 - federated identity models. *Privacy Law and Policy Reporter*, 11(1), August 2004. <http://search2.austlii.edu.au/au/journals/PLPR/2004/23.html>.