

Selected Privacy and Security Issues in Digital Government

IT GOVERNANCE AND CIVIL SOCIETY RESEARCH NETWORK
INFORMATION TECHNOLOGY AND INTERNATIONAL COOPERATION (ITIC) PROGRAM
SOCIAL SCIENCE RESEARCH COUNCIL
http://www.ssrc.org/programs/itic/governance_report/memos_gov.page

OCTOBER 2004

William J. McIver, Jr.
P.O. Box 907
Postal Station A
Fredericton, NB E3B 5B4
Canada

Member:

- ACM Special Interest Group on Computers and Society
- Community Informatics Research Network (CIRN)
- Communication Rights in the Information Society (CRIS)
- Computer Professionals for Social Responsibility (CPSR)
- IEEE Computer Society Special Interest Group on Social Implications of Technology

e-mail: wmciver@acm.org

1. Introduction

Digital government can be defined as the civil and political conduct of government using information and communication technologies (ICT). This includes the provisioning of services and the management of legislative processes. Such technologies can empower citizens with greater access to services and more flexible and effective means of participating in government, leading to improved citizen-government interaction and – hence -- an overall improvement in society. These interests must be balanced, however, with both security and privacy concerns.

Two distinct yet interrelated goals that are critical to the provisioning of digital government are security and privacy. Privacy is a social condition that is considered desirable in many conditions. Security mechanisms enable privacy. This memo examines selected issues relating to privacy and security in digital government, in particular it discusses the policy shift away from the traditional view of non-repudiation that has been brought about by technical authentication mechanisms and developments in security policy since September 11th, 2001. The next section of this paper presents a taxonomy of system architectures in digital government as background. Selected technical aspects of security and privacy are then presented. Finally, policy aspects of privacy and security are discussed.

2. Background

A wide spectrum of technologies – both hardware and software -- can be considered to exist within the category of digital government systems. These include technologies that “externalize” government by enabling citizens or government officials to interact with governmental processes, and those technologies that perform internal governmental processes. We will refer to the former type of digital government technologies as externalizing systems and the latter as internal systems. The prime examples of externalizing digital government systems technologies are the Web-based services that have become prominent in the past few years. Internal digital government systems technologies include novel applications of computing techniques in geographic information systems (GIS), database management and image processing to solve critical tasks within government agencies. Of course, many externalizing systems employ the services of internal systems. The contributors to this volume discuss examples of both externalizing and internal systems technologies.

The architectures of systems in both the categories of externalizing and internal digital government systems are in most cases database-centric. It is, therefore, necessary to discuss security and privacy in digital government technologies along both the dimensions of system architectures and data management. These are discussed below.

3. System Architectures

In this section, we discuss digital government system architectures within each part of our taxonomy of externalizing and internal systems.

3.1 Externalizing systems

The dominant vision of externalizing digital government systems has become -- like many other areas of the information technology (IT) sector -- Web-centric. Commercial Web service offerings have clearly raised citizens’ expectations of the level of service provided by government agencies over the Web [8]. Digital government systems can generally be characterized along two dimensions: the architectural relationship they have with their clients and the type of service they are capable of providing for their clients. Architectures include intranets to support intra-governmental processes, public network access to facilitate government-citizen interactions, and extranets for supporting interactions between government

and non-governmental organizations (e.g. government-to-business).

Four basic types of Web architectures are seen among current externalizing digital government systems, each corresponding to one of four levels of service [1]:

Level 1 Externalizing Services. Level one services provide one-way communication for displaying information about a given agency or aspect of government.

Level 2 Externalizing Services. Level two services provide simple two-way communication capabilities, usually for simple types of data collection, such as the registration of comments with government agencies.

Level 3 Externalizing Services. Level three services extend on level two services to provide the ability to carry out complex transactions that may involve intra-governmental workflows and legally binding procedures. Examples include voter and motor vehicle registration.

Level 4 Externalizing Services. The fourth level of service is characterized by the emergence of government portals that seek to integrate a wide range of services across a whole government administration. The eCitizen portal developed by the government of Singapore is a prime example of this type of system (see <http://www.ecitizen.gov.sg>).

A number of notable level 3 externalizing services have evolved in the past few years. The e-petitioner system of Macintosh, Malina and Farrell [19], supports citizens in the function that most represents democratic governments: the process of decision making through voting. E-petitioner allows citizens of Scotland to create, view, discuss, sign, and submit petitions to the Scottish parliament. Han, Kunz and Law [14] have developed an on-line system for testing the compliance of building and facilities designs with the Americans with Disabilities Act. Karr et al. [17] have developed a Web-based system designed to provide citizen access to statistical data, such as agricultural data, in a manner that protects the confidentiality of those data. Zhang, Zhu and Mark [26] have developed the WebView system, which provides officials and citizens efficient access to very large geographic image databases.

Three representative level 4 externalizing services are the WebDG system by Bouguettaya et al. [7], the Italian National Public Administration Network and domain-specific Cooperative Information Systems (CIS) [5], and the Tunisian Multi-Service Network [6]. WebDG consists, in part, of Web-based facilities that allow citizens to more easily access information and

processes across related and often geographically disparate social service agencies. WebDG is capable of supporting level 4 services in that it performs ontological and process integration between different government agencies. Both the Italian and Tunisian systems support Web-based externalization of services for government officials within an overall framework that seeks to integrate ministries across the whole government.

3.2 Internal systems

A wide spectrum of technologies can be considered to fall within the category of internal digital government systems, including those that perform tasks common to large organizations, such as financial management, document processing, and communications (e.g. e-mail). Such systems fall generally into two categories:

Integrative and communicative systems: These are systems that provide support for inter-agency (or ministry) integration and cooperation.

Domain-specific processing and knowledge management systems: These are systems that provide support for processing and interpretation of data within ontologies that are unique to government, such as agricultural statistics, data used by law enforcement agencies, social services policies (i.e. rules) and data, and geographic images from government geological surveys.

Several notable integrative and communicative systems have been developed in the past few years. The WebDG system discussed above in the context of externalizing services also features internal digital government functions designed to integrate information and processes across disparate social service agencies. This capability is critical when citizens require a set of related services, each provided by separate agencies (e.g. financial assistance together with childcare). Atluri et al. [3] are developing a decentralized workflow management system called DWFMS, which is designed to support inter-agency workflows involved in the registration of businesses. Ambite et al. [2] are developing the DGRC System, which is designed to capture and integrate statistical information across different government agencies, each represented by different ontologies. Golubchik is developing a system called Bistro, which supports scalable uploading of documents (e.g. tax returns) – with or without deadlines -- across the Internet [13].

Several notable domain-specific processing and knowledge management systems have been developed in the past few years. The systems of Han, Kunz and Law; Karr et al.; and Zhang, Zhu

and Mark – all discussed above in the context of externalizing services – can be classified in this category. In addition, Hauck, Chau and Chen [15] have developed a collection of software technologies called COPLINK, which enables “information sharing and criminal analyses within and between law enforcement agencies.”

Of course, it is possible for systems to span these two categories. Also discussed above in the context of externalizing services, the National Public Administration Network and domain-specific Cooperative Information Systems (CIS) of Batini et al. [5] are components of an overall framework that span the categories of integrative and communicative systems and domain-specific processing and knowledge management. This framework, developed by Italy’s Authority for Information Technology in the Public Administration (Autorità per l’Informatica nella Pubblica Amministrazione) or AIPA is designed to “increase organization efficiency and overall effectiveness of administrative actions” by facilitating greater inter-ministry cooperation through software-centric solutions.

4. The Need for Security and Privacy

The need for security mechanisms is found within both the categories of externalizing and internal systems. Each category of system may be faced with supporting some or all of the following tasks:

- presenting confidential data, as in externalizing services at levels 1 through 4;
- collecting confidential data, as in externalizing services of levels 2 through 4;
- performing legally binding services, as in externalizing services of levels 2 through 4; or in
- managing any type of sensitive data within internal government systems.

The need for confidentiality may be a function of legal requirements for handling citizen data that are of a personal nature or of the handling of data whose disclosure can in some way threaten the operation or security of citizens or government.

4.1 Technical Perspectives on Security

Security services are necessary in digital government systems to enable data privacy, privacy of communications, and authentication. Many collections of government data contain information that is sensitive with respect to citizens or the government itself. This type of information must

obviously be managed using cryptographic methods to increase the probability that only authorized parties can view it. The communication of such data via digital government systems must also be protected from unauthorized eavesdropping.

Authentication and non-repudiation

Authentication – beyond simple identity verification (e.g. password-based logins) – is becoming increasingly necessary as more complex transactions are being handled by digital government systems. These types of transactions include the level 3 and level 4 externalizing services discussed above. Necessary authentication services include the following:

Authentication and Digital Signatures: It must be possible to verify the identity of someone or the ownership of information created by, transmitted through, or stored in a digital government system during the processing of a transaction.

Repudiation/Non-repudiation: A digital government system must have a method for authenticating the originator of a transaction in a way that is verifiable by third parties, and in a way that does not allow the originator to later refute that they originated the transaction.

Certification Authorities: It is necessary to bind the identity of the originator of a transaction in a way that is verifiable by a third party together with any information associated with authentication, non-repudiation or any other security processes during a transaction. Such information includes public keys and digital certificates. If, for example, a user or process presents a digital certificate, its validity and ownership by that user or process must be verifiable.

See Rivest, Shamir and Adelman [22] for a basic introduction to public key encryption.

Database Security

A database system might be configured using standard database management system security mechanisms to restrict access to individual records containing confidential data; however, it might still be possible to deduce confidential information through the creative application of statistical queries over that same data if no special precautions are taken. This problem area is referred to as statistical database security.

Statistical database security is a critical security issue in digital government systems. Statistical queries apply aggregate statistical measures (e.g. averaging, locating a mean value for an attribute, or finding a maximum value for an attribute) to collections of data.

Suppose, for example, a government agency were to store statistical data about a population – say home owners in Albany, New York – but allowed only aggregate queries over sensitive attribute values such as income and disallowed access to attributes such as name. A user might still be able to deduce an individual’s income by submitting a query for average income while restricting other attribute values such that the targeted individual’s record is isolated (e.g. by address, occupation, or some combination of attributes). This issue and effective countermeasures are discussed in greater depth by Karr et al. [17] See also Joshi, Ghafoor, Aref, and Spafford [16] for a comprehensive security model for digital governments.

4.2 Policy Perspectives on Security

Policies are sets of principles and plans of action that are designed to achieve an associated set of goals. Policy making with its relationship to a set of goals can be, as the well-known sociologist and public planner Herbert Gans declared, a “rational” process in that “policies can be proved to implement the goals being sought” [12]. There are three major areas in which digital government policymaking has been focused:

Government transformation: These are policies that help transform governmental organizations to make them more receptive to the deployment of digital government systems.

Public infrastructure: These are policies that guide the transformation of public infrastructure to facilitate the deployment and use of digital government systems.

Social and economic issues: These are policies that address the social impacts or economic issues that arise in the development, deployment and use of digital government technologies.

Security and privacy issues permeate each of these policy areas. It is necessary to enable data privacy and authentication in digital transactions between citizens and government and within government. Security is traditionally viewed as a technical issue, whereas privacy is viewed as an often desirable and expected social condition that can be enabled by security. Privacy is, thus, addressed as a goal to be met through social policies and laws that guide the deployment and use of technologies. These social policies may in turn mandate certain technical policies.

Data privacy and privacy of communications

Data privacy and privacy of communications are the aspects of privacy that are key in digital government. Laws and policies have evolved in many countries that address data privacy and privacy of communications. Though in many countries, it should be noted, citizens do not have a general right to privacy. That is, a right that explicitly encompasses all aspects of privacy: bodily privacy, territorial privacy, data privacy and privacy of communications. Banisar [4] provides a comprehensive examination of privacy laws across the world.

Data privacy policies are concerned with both the collection and processing of data. A preference-based model is often employed to describe the privacy status of data that are collected from users. There are two variations of this model: data are either assumed to be private or they are not assumed to be private. Users should be entitled to either opt in to or opt out of the respective privacy regime. This, of course, does not address the issue of enforcing data privacy.

Countries employ two models of data privacy enforcement relevant to digital government. Some countries have passed laws that focus narrowly on the conduct of government agencies with regard to data privacy. Such laws generally require the government to protect personal data that it collects from citizens and to require agencies to justify (internally) the transfer of and use of such data by other agencies. The U.S. Privacy Act of 1974 is an example of such a law. Other countries, such as the members of the European Union (E.U.), have in the past taken a more comprehensive approach by providing data privacy protection laws that encompass both private and public sectors, and that provide for a centralized agency to enforce these laws. Countries have also handled communications privacy using these models.

The differences between these two models of data privacy enforcement can pose potential conflicts in an international context. How, for example, are the data regarding a citizen involved in immigration to be handled between two countries that have different data privacy standards? Commerce, which is regulated by governments, is also subject to this type of conflict. The E.U. and the U.S., as a result of each having incongruent data privacy laws, were forced to negotiate a “safe harbor” agreement that addressed the handling of personal data that are transmitted between the U.S. and E.U. member states [4].

A working group within the World Wide Web Consortium (W3C) is developing a standard called P3P (Platform for Privacy Preferences Project) designed to ease the publication by Web

sites of their data privacy policies and the interpretation by users or software agents of those privacy policies [24]. Under this standard, Web sites encode their privacy policies according to the P3P protocol, which provides for encoding policies using XML-based elements. The P3P protocol also defines, among other things, the process by which a privacy policy is located and the semantics of P3P elements. As of this writing, the P3P specification had reached the Last Call Working Draft for version 1.0.

Authentication and non-repudiation

Authentication as a digital government policy issue is concerned with the use of sound methods of verifying identification and achieving non-repudiation – just as it is from a technical perspective. Digital signatures and encryption provide sound technical approaches for addressing both concerns. Governments, such as the E.U., and various states within the U.S., have in recent years passed laws that make digital signatures legal forms of authentication and that, in some cases, allow government to serve as a certification authority for such signatures [11, 23].

Non-repudiation policies address a person's rights and abilities to refute a claim that a signature belongs to them. In other words, under sound conditions for non-repudiation, a person would be legally and technically unable to repudiate a signature they made. From a technical perspective, digital signatures created using public key encryption can implement non-repudiation because a message and its reputed sender's public key can be used in combination to verify that a digital signature used to "sign" the message was created using both the sender's private key and the message. The traditional legal concept of non-repudiation presents conflicts with this technical concept of non-repudiation, however.

Under the traditional concept, a person can repudiate a signature on a document by claiming that it is either a forgery or that the signature is not a forgery, but was obtained illegally (e.g. through coercion). Non-repudiation can be achieved by having a third party, such as a notary, witness the creation of a signature. Another conflict has arisen over the burden of proof for non-repudiation. The burden of proof under traditional non-repudiation has been the receiver of the signature, not the alleged signatory. Within the digital realm, however, the legal meaning of non-repudiation has been evolving such that an alleged signatory either has the burden of proof or they no right of repudiation at all [20]. Clearly, this is an issue that must be resolved in the context of digital government, as digital signatures are certain to become more commonplace in citizen-government interactions.

National and International Security Issues

The terrorist events in the U.S. of September 11, 2001 is arguably the most glaring and tragic example of a set of events that has long been the focus of policy debates about balancing security with citizens rights to privacy and freedom of information. This has resulted in renewed calls for governments to take more in-depth approaches to on-line security.

The European Parliament has recently made radical changes in its data privacy policies in response to the so-called “war on terrorism.” Police forces in E.U. member countries were recently given permission to access the telephone and Internet usage records of all of their citizens [21]. Access to such records is mediated by the requirement that police obtain a warrant prior to monitoring communications or reviewing of records of communications.

The concept of digital government is for many people premised upon the notion that citizens have the right to access the information that their government produces. Unfortunately, acceptance of this concept has been weakened by the events of September 11th. Even the routine publication of unclassified information via the Web has been called into question by some policymakers. Many argue that even unclassified information, such as the location of public points of interest, could aid people in perpetrating terrorist acts.

Spafford argues that security for governments must begin with the procurement of technologies to be used [18]. In conjunction with procurement, many are now calling for the use of open source systems on the theory that security flaws can more easily be identified.

5. Conclusions

The civil and political conduct of governmental functions through the use of information and communication technologies has revolutionized and, arguably, improved citizens’ interactions with their governments. These capabilities, however, raise serious security and privacy issues that must be addressed from both technical and policy perspectives. This paper examined selected technical and policy issues relating to privacy and security in digital government. In particular, the paper discussed the policy shift away from the traditional view of non-repudiation that has been brought about by technical authentication mechanisms and major developments in security policy since September 11th, 2001.

References

1. "No gain without pain." *The Economist*, June 24, 2000.
2. Ambite, José Luis, Yigal Arens, Walter Bourne, Steve Feiner, Luis Gravano, Vasileios Hatzivassiloglou, Eduard Hovy, Judith Klavans, Andrew Philpot, Usha Ramachandran, Kenneth A. Ross, Jay Sandhaus, Deniz Sarioz, Rolfe R. Schmidt, Cyrus Shahabi, Anurag Singla, Surabhan Temiyabutr, Brian Whitman and Kazi Zaman. (2002). *Data Integration and Access: The Digital Government Research Center's Energy Data Collection (EDC) Project*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
3. Atluri, Vijayalakshmi, Soon Ae Chun, Richard Holowczak, Nabil R. Adam. (2002). *Automating the Delivery of Governmental Business Services Through Workflow Technology*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
4. Banisar, David. (2000). *Privacy & Human Rights 2000: An International Survey of Privacy Laws and Developments*. Washington, D.C., USA: Electronic Privacy Information Center and London, UK: Privacy International. <http://www.privacyinternational.org/survey/>.
5. Batini, Carlo, Elettra Cappadozzi, Massimo Mecella, Maurizio Talamo. (2002). *Cooperative Architectures: The Italian Way Along e-Government*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
6. Boudriga, Nouredine and Salah Benabdallah. (2002). *Laying out the Foundation for a Digital Government Model Case Study: Tunisia*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
7. Bouguettaya, Athman, Mourad Ouzzani, Brahim Medjahed, and Ahmed K. Elmagarmid. (2002). *Supporting Data and Services Access in Digital Government Environments*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
8. Cook, Meghan E. (2000). *What Citizens Want From E-Government: Current Practice Research*. Center for Technology in Government. October.
9. Diffie, Whitfield and Susan Landau. (2002). September 11th Did Not Change Cryptography Policy. *Notices of the AMS*. Volume 49, Number 4.
10. eCitizen. Singapore's Citizen Service Portal. <http://www.ecitizen.gov.sg>.
11. European Union (EU). (1999). Directive 1999/93/EC Of The European Parliament And Of The Council Of The European Union of 13 December 1999 on a Community framework for electronic signatures. <http://europa.eu.int>.
12. Gans, Herbert J. (1993). *People, Plans, and Policies: Essays on Poverty, Racism, and Other National Urban Problems*. New York: Columbia University Press.
13. Golubchik, Leana. (2002). *Scalable Data Collection for Internet-based Digital Government Applications*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
14. Han, Charles S., John C. Kunz and Kincho H. Law. (2002). *Compliance Analysis for Disabled Access*. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.

15. Hauck, Roslin V., Michael Chau & Hsinchun Chen. (2002). COPLINK: Arming Law Enforcement with New Knowledge Management Technologies. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
16. Joshi, James B. D. Arif Ghafoor, Walid G. Aref, and Eugene H. Spafford. (2002). Security and Privacy Challenges of a Digital Government. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
17. Karr, Alan F., Jaeyong Lee, Ashish P. Sanil, Joel Hernandez. (2002). Web-based Systems that Disseminate Information from Data but Protect Confidentiality. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
18. Krim, Jonathan. (June 19, 2002). The Internet Gets Serious. *Washington Post*. p. H1.
19. Macintosh, Ann, Anna Malina, and Steve Farrell. (2002). Digital Democracy through Electronic Petitioning: e-petitioner. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.
20. McCullagh, Adrian and William Caelli. (August 2000). Non-Repudiation in the Digital Environment. *First Monday*, volume 5, number 8. URL:
http://firstmonday.org/issues/issue5_8/mccullagh/index.html.
21. Millar, Stuart. (May 31, 2002). Europe votes to end data privacy: Law will allow police to spy on phone and net traffic. *Guardian Unlimited*.
22. Rivest, R., Shamir, A. and Adelman, L. (1978). "On Digital Signatures and Public Key Cryptosystems." *Communications of the ACM*, Vol. 21, No. 2, February.
23. State of California. (1995). Digital signatures, AB 1577, chapter 594., Chaptered October 4, 1995.
24. World Wide Web Consortium (W3C). (2001). The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. W3C Working Draft 28 September 2001.
<http://www.w3.org/TR/2001/WD-P3P-20010928>.
25. Zakon, Robert H. (2001). Hobbes' Internet Timeline v5.4. <http://www.zakon.org>.
26. Zhang, Aidong, Lei Zhu, and David Mark. (2002). WebView: A Globally Accessible Geographic Image Database Environment. IN W. McIver and A. K. Elmagarmid (eds.) *Advances in Digital Government: Technology, Human Factors, and Policy*. Boston: Kluwer.