eGovernment & Internet Security: Some Technical and Policy Considerations

Luis F. Luna-Reyes and J. Ramón Gil-García
Center for Technology in Government
1535 Western Av., Albany, NY 12203
lluna-reyes@ctg.albany.edu jgil-garcia@ctg.albany.edu

Abstract

The purpose of the present essay is to discuss some technical and policy considerations of Internet security in the context of electronic government applications. The initial sections of the paper are oriented to describe the main security concerns, their relative importance in different categories of eGovernment applications, and some of the current security technologies. In the final sections, a preliminary assessment of the adequacy of the technologies to each group of applications is offered, highlighting some implications on the development of electronic government and policy.

1. Introduction

Internet security has become an important topic to system administrators, policy makers, computer scientists, and almost anyone who uses a computer. Private corporations, governments, and non-governmental organizations are increasing the use of the Internet to either increase their productivity, reduce their costs, improve their services, communicate to the public or promote organizational change. However, the resulted increasing number of electronic transactions is also making this medium an increasingly attractive place for crime, as well as security, and privacy violations.

The purpose of the present essay is to discuss some key technical and policy considerations of Internet security in the context of electronic government applications, and it is organized in four sections. The first section constitutes a brief description of the security problem, and the main security concerns. The next section describes the main Internet applications in government, and the security concerns in this context. The third section is devoted to talk about the technical and practical limits of some of the most important security technologies. The last section outlines some implications of these limits on the development of electronic government and policy.

2. Internet Security

Internet security is a problem of significant dimensions. The 2002 annual survey on Computer Crime reported that 90% of the respondents detected security breaches, with an associated financial loss of more than $450 millions during the previous year. The point of attack reported was the Internet connection in 74% of the cases, and 33% was from the internal system (Power, 2002).

In general, security process in the Internet requires the implementation of the same processes to establish security in a physical system: confidentiality, authentication, integrity, non-repudiation, authorization, privacy, and written control policies (Busta, 2002; Kleckner, 2002). Confidentiality refers to the fact that any message is only accessible to its sender and recipient, preventing a third party to read or listen to the message. The main purpose of authentication is to verify that people or organizations engaged in a transaction are who they are claiming to be. Keeping the integrity of communications involves processes to assure that the message received is the same message sent by a user. Non-repudiation entails mechanisms to proof that an actor involved in a transaction was the actual origin of the message. Authorization includes the mechanisms and processes of assigning different levels of access and permissions to users of a system or service. Keeping information gathered by an agency from inappropriate disclosure and use is the main purpose of privacy. Finally, all the processes described so far should be properly documented and made public in a comprehensive set of policies and procedures.

Each eGovernment application entails different levels of risk and security concerns, and each of them has to be analyzed separately by policy makers and managers in order to identify threats, costs, and the best way to approach every security need (Irvine, 2000).

3. Security Issues in eGovernment Applications

Electronic Government applications range from electronic portals developed to provide basic information or services to citizens (LaVigne, 2002; Zweers and Planqué, 2001) to applications to electronic voting (Larsen, 1999; Rubin, 2002), and citizen participation in the rule-making process (Fountain, 2003). A recent review to the emerging literature in electronic government suggests that the diversity of eGovernment applications can be grouped in 4 main categories (Gil-García and Luna-Reyes, 2003): Electronic Services (E-Services), Electronic Management (E-Management), Electronic Democracy (E-Democracy), and Electronic Policy (E-Policy).

E-Services applications are those relating to the delivery of information or services to the citizen. Desirable features of these applications are the organization of the information according to the "customer profile", the capability to allow a "customizable" experience, and the ability to "make transparent" to the user the agency or level of government with which he is dealing (Zweers and Planqué, 2001). The main issues from the security point of view are the verification of the identity of the server computer (Authentication), the integrity of the message, confidentiality, and the privacy associated with the transmission of the information. Although the authentication of the user is also desirable, simple user authentication mechanisms such as passwords are cost-effective for most of these applications.

E-Management applications include those related to the improvement of government internal operations inside a single instance of government or across agencies (Grönlund, 2001; Holmes, 2001). Many of these applications require a significant change in government processes, including a more intense interaction among government agencies through database integration or intercommunication. Protecting the integrity of data, guaranteeing the privacy of the citizens, and controlling the access to data only to the authorized agents are undoubtedly the most relevant security issues in this kind of applications. The integration of databases calls for a clear definition of information ownership and access. Finally, for transactions and services among government agencies and private corporations such as procurement, authentication and non-repudiation becomes important issues.

E-Democracy is mostly associated with electronic voting (Larsen, 1999; Rubin, 2002), but it is also associated with citizen participation in the processes of policy making, promoting and preserving the democratic values (Fountain, 2003). These applications pose the most complex set of security concerns for their successful implementation. E-Democracy applications must include the same elements of security associated with E-services in terms of authentication, integrity, confidentiality, and privacy of the communications. However, some applications call for better approaches to user authentication while assuring their anonymity.

Finally, E-Policy is related to the design of public policies that facilitate and promote the development of the information society. Technology is changing the structure of social organizations and their interaction. This new structures require an adjusted policy framework to facilitate the interaction and promote democracy and equal opportunities to the different constituencies. From the authors' point of view, policy thought about privacy and access to the information, and the tension associated with these two important issues are the key elements for E-Policy. Monitoring of Internet transactions by some government agencies provides a good example of the tension between these values. On one hand, privacy concerns of Internet users create pressures to reduce monitoring to a minimal level. On the other hand, threats to security breaches promote a closer monitoring of the activity.

4. Technical and Practical Limits to Internet Security

The present section constitutes a description of some of the most common security technologies and their limitations. In general, the authors' perception is that hackers and security administrators are engaged in a competitive war with an escalation behavior. As a result, the sophistication of both the security technologies and the nature of the attacks are continuously growing. Every technology needs to be supported by proper strategies, policies, business processes, and reinforcing procedures.

There are three different ways of authentication technologies. The first set of technologies is based in something the user *knows*, like passwords or user names. The second authentication category uses something the user *has*, such as smart cards, tokens or digital certificates. Finally, authentication technology could be built in terms of something the user *is*, like fingerprints, retinal scans or other biometrics. None of these technologies is entirely secure. Even the combined use of them is not perfect. On this way, some experts recommend to combine these technologies with the traditional involvement of multiple actors in important control points of the business process (Kleckner, 2002).

Authorization to network resources is enforced by the use of software and hardware, which are the equivalent to a building main entrance guard. However, the original gate-keeping principle is no more enough to protect the resources to certain automated attacks (Rubin, 2002). On this way, the actual systems attempt to detect attacks by the application of statistical techniques to monitor the activity of the organization network. These techniques offer a reasonable secure solution to intrusion problems.

Modern cryptography offers a series of technologies that can be used to satisfy several security concerns. Although cryptographic techniques were used initially to facilitate confidentiality and integrity of communications, recent uses (public key infrastructure, digital certificates, and digital signatures) include authentication and non-repudiation (Abrams and Podell, 1995). In a very simple way, encryption is a process that consists in scrambling the original message in an undecipherable form (Busta, 2002). Each encryption scheme has its own capabilities and limitations, and none of them is 100% secure.

Finally, the human element involved in the implementation of any security system makes all of them vulnerable. Human error is identified as one of the main security threats and vulnerabilities (Irvine, 2000) in the form of imperfect designs, bad programming practices or user decisions.

5. Implications for E-Government

The implications of the security limits in the Internet have a different impact according to the type of eGovernment application. Technical limitations force trade-offs between costs and benefits. Managers have to design cost-effective strategies that reach a balance between productivity and risk (Irvine, 2000). The diversity of constituencies, on the other hand, creates pressures to protect privacy or to guarantee access to the information. Although the appropriate balance has to be analyzed and discussed by the different actors involved in each application, this section of the paper presents some general considerations that could be taken as a starting point for the discussion.

The current state of security systems offers an acceptable level of authentication, privacy, integrity, and confidentiality to most of the applications in e-Services. The expected benefit from tampering a transaction is in general much lower than the investments needed to accomplish it. However, the consideration of security issues in the back-end of the processes has to be carefully analyzed for each particular case. That is to say, servers keeping transaction information and communications among them are much more attractive targets for the attacker.

Most of the e-Management applications can also rely on the use of the current security technologies. The Public Key Infrastructure and the current monitoring systems provide a reasonable level of security for most of these applications. However, the human side provides most of the challenges for this area.

Efforts in the Department of Labor, among others, constitute a good example of organizational involvement in the development of an agency-wide security strategy (Armstrong, 2002).

In general, e-Democracy applications are the most vulnerable to security risks. The costs, though difficult to estimate, could be very high. Although there are several experiments with different levels of success (Larsen, 1999), the current status of hardware and software does not provide an acceptable level of security for this kind of application, which in some cases requires anonymity (Rubin, 2002).

From the authors' point of view, e-Policy is the area with most opportunities of development, but also with bigger challenges. The security function has to be analyzed and redesigned as part of an integral process, involving social, managerial, and political considerations. The result of this design will impact in a significant way the rest of the areas of eGovernment.

6. Conclusion

Absolute security is unattainable. However, it is possible to obtain effective results by changing some of our beliefs and working in the development of comprehensive security systems, which starts with the conversation about the business processes involved in the application to identify key control points on the application. The success of the initiative involves good management, enforced procedures, and the adequate technical tools, with an appropriate policy framework. Security policies should not only consider the control of computer systems and networks, but physical security, administrative, legal and organizational controls too. In addition, the adequate balance of information policy values embedded in a security system for any eGovernment application is an *ad hoc* social and political decision.

7. References

Abrams, M. D. and Podell, H. J. (1995), "Cryptography", in Abrams, M. D., Jajodia, S. and Podell, H. J. (Eds.), *Information Security: An Integrated Collection of Essays* IEEE Computer Society Press, Los Alamitos, CA.

Armstrong, A. (2002),"E-Government Work Force Planning: A Pilot Study", *Journal of Government Financial Management,* Vol. 51 No. 2, pp. 32-35.

Busta, B. (2002),"Encryption in Theory and Practice", *The CPA Journal,* Vol. 72 No. 11, pp. 42-48.

Fountain, J. E. (2003),"Prospectus for Improving the Regulatory Process Using E-Rulemaking", *Communications of the ACM,* Vol. 46 No. 1, pp. 63-64.

Gil-García, J. R. and Luna-Reyes, L. F. (2003), "Towards a Definition of Electronic Government: a Comparative Review", in A.Mendez-Vilas, Mesa-González, J. A., Guerrero-Bote, V. and Zapico-Alonso, F. (Eds.), *Techno-Legal Aspects of Information Society and New Economy: an Overview*, Vol. I Formatex, Badajoz.

Grönlund, Å. (Ed.) (2001) *Electronic Government: Design, Applications, and Management,* IDEA Group Publishing, Hershey, PA.

Holmes, D. (2001), *e.gov. e-business Strategies for Government,* Nicholas Brealey Publishing, London.

Irvine, C. E. (2000), "Security Issues for Automated Information Systems", in Garson, G. D. (Ed.) *Handbook of Public Information Systems* Marcel Dekker, New York.

Kleckner, J. E. (2002),"E-Security 101", *AFP Exchange,* Vol. 22 No. 3, pp. 54-56.

Larsen, K. R. T. (1999),"Voting Technology Implementation", *Communications of the ACM,* Vol. 42 No. 12, pp. 55-57.

LaVigne, M. (2002),"Electronic Government: A Vision of a Future that is Already Here", *Technology and Legal Practice of the Syracuse Law Review,* Vol. 52 No. 4.

Power, R. (2002),"2002 CSI/FBI Computer Crime and Security Survey", *Computer Security Issues and Trends,* Vol. 8 No. 1.

Rubin, A. D. (2002),"Security Considerations for Remote Electronic Voting", *Communications of the ACM,* Vol. 45 No. 12, pp. 39-44.

Zweers, K. and Planqué, K. (2001), "Electronic Government. From an Organizational Based Perspective Towards a Client Oriented Approach", in Prins, J. E. J. (Ed.) *Designing E-Government. On the Crossroads of Technological Innovation and Institutional Change* Kluwer Law International, The Hague, Netherlands, pp. 91-120.