ISSN No. 0976-5697

Volume 5, No. 1, Jan-Feb 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

An Extended Security Framework for E-Government

K .Seena Naik*
Dept of CSE, S K University Anantapur, India
seenasuna558@gmail.com

Dr G.A Ramachandra
Dept of CSE, S K University Anantapur, India

M V Bramhananda Reddy
Gitam University, India
bramhareddy999@gmail.com

Abstract: Many governments have delivered their services in ways that meet the desires of the citizens and businesses they serve, enabling them to interact securely in places and at times that are convenient for them. E-government is one of the most important achievements of the Internet. Successfully implementing e-government requires a level of trust on the part of all transaction parties. There are several security techniques and tools that have been developed in the scope of e-commerce. However, development of secure e-government systems requires a comprehensive model for security that can by implemented during the life cycle of the project. This paper introduces an enhanced security framework that is designed especially for e-government systems. Such a security framework is an essential tool that can be used by decision makers and designers of e-government systems.

Keywords: e-government, security framework, security goals, security policies

I. INTRODUCTION

The twenty first century has rapid growth in the use of the Internet and its technologies. This causes a big change in the management role in both public and private sector. E-government, e-commerce, e-management are new concepts that have received an increasing interest from both the researchers and practitioners in many countries, especially the developed. Developing countries, on the other hand, are trying to catch up in this field. Governments are trying to deliver their services in ways that meet citizens, employees and businesses needs effectively and efficiency. The Internet allows a quick update and access to any information any time the user wants. E-government is the most important accomplishment of Internet. There is, however, one main downside that is occurring within each process of e-government, namely security. E-government processes and services must be secure as technology will allow and the users must follow the policies set to make their own actions safe. One of the primary challenges and obstacles to successful deployment and operation of e-government is security

[1]. In this paper the authors will propose an extended security framework for e-government projects. This framework is a document with a high level expression of security requirements and expands upon the security statements in e-government. The main aim of this framework is ensuring that all e-government services and processes are secure. The rest of the article is organized as follows: section 2 introduces some of the security threats to e-government. Section 3 highlights some of the challenges to e-government in the context of system integration. Section 3 presents the extended security framework for e-government. Finally, section 4 concludes the article and outlines some future work.

II. SECURITY THREATS

From a technical point of view, there are three types of threats that are found in both e-government and e-commerce [2]: unauthorized access which affects confidentiality, unauthorized change or modification to the information which affects the integrity of information, and the threat that affects the availability of both information and services. There is also a fourth type, namely the threats against accountability such as denying involvement in a transaction. These threats can be further classified into three classes: inter-communication which has two types of threats: passive manipulations, which cannot be proven such as analysis of web traffic, and active threats which can be recognized but cannot be prevented such as modification in message content. The second class is intra communication threats, which are caused by the communication participants themselves such as computer fraud and computer forgery. The last class of threats is related to systems or resources. An example of this threat is Trojan horse, viruses and flooding.

Knowing threats from technical point of view is not enough. Therefore, security threats should be investigated from non-technical point of view as well.

III. SYSTEM INTEGRATION IN E-GOVERNMENT

E-government requires cross-agency cooperation because of functional needs for scale, consistency, and integration. Within the confines of the e-government community, integration describes those processes that deliver information and services to users at all levels. Advances in information and communication technologies, and in the ability to share and deliver this information, are revolutionizing the way business is done in the e-government community. As a result, the concept of integration is evolving and expanding as quickly as the changes in the technology that drive it. There are several challenges that face effective and efficient sharing of information between government agencies on the one hand, between governments, and between governments and businesses and citizens. Such challenges range from trust transparency in information system design, to ethical and legal issues when integrating information systems [3]. This justifies the need for a comprehensive security model that takes into consideration the systems integration element.

IV. AN EXTENDED SECURITY FRAMEWORK

The e-Government framework is a guideline used by government organizations and businesses working with the government. The security framework introduced in this section is an extension of the framework published by the British Standards Institute (BSI) [4], which details the conception, specification and implementation of e-government services. This framework can be used to measure the security level for the e-government websites.

The main components of the framework are shown in figure

a. The framework considers all aspects of e-Government security—the people, processes and technologies. This layered approach to e-government security combines strong policy management and enforcement, which should drive the security requirements of e-Government systems. The proper elicitation and management of security requirements is a key to successful development of secured e-government systems [5].

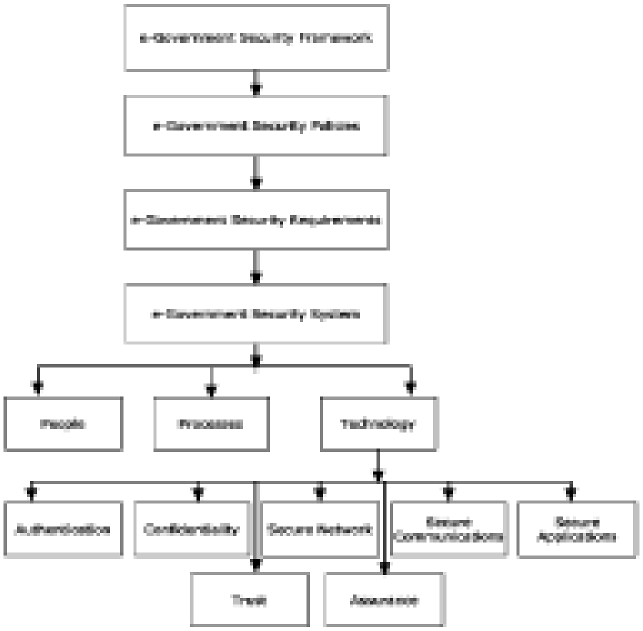
e-Government Security Framework
e-Government Security Policies
e-Government Security Requirements
e-Government Security System
People
Processes
Technology
Authentication
Confidentiality
Secure Network
Secure Communications
Secure Applications
Trust
Assurance

Figure: 1 A Comprehensive Security Framework

The People component refers to the people using e-Government. Awareness programs need to be carried out by governments to make sure that the users of the e-government are aware of the security problems and their implications.

The Processes component refers to the processes that govern e-Government use, typically administered through the security policies and procedures. Technology is used to enforce the e-Government security, but is only as good as its weakest link. For technology to enforce the security, it must be multi-layer and properly implemented at each level. The technology subcomponents are briefly described below:

(a). Authentication*:* Identified users uniquely and unambiguously make sure that only the authorized person can access to the system.

(b). Confidentiality: Only authorized persons can access the information. So information is stored securely and not disclosed to unauthorized persons or processes.

(c). Secure Applications: Make sure that the e-government services applications are designed, developed, configured and operated in a secure and robust manner.

(d). Secure Network: Protect information and transaction from any kind of attack.

(e). Secure Communications: Protect information while in transit from tampering or disclosure.

(f). Trust: Ensure that transactions are traceable and accountable to authenticated person and cannot subsequently be denied.

(g). Assurance: Make sure that trust is included in the implementation of security elements.

This e-government security framework, depicted in figure 1, provides key guidance to service providers wishing to gain the trust and confidence of their users. It also ensures that security technologies put in place meet the security requirements. Though not depicted in the figure above, the security requirements of any e-government system should analyze the threats and attacks that may face it. This is usually integrated into the secure application development using a modern software risk analysis methodology.

V. CONCLUSION

The Internet has become both the source of information and source of threats. This paper introduced a comprehensive security framework that addresses the key components to secure e-government services and operations. Such a framework helps governments to effectively incorporate security into e-Government systems by considering all key security elements. Future work will investigate how such a framework would be applied in a real-world project.

VI. REFERENCES

[1]. M. Hwang, et al., “Challenges in e-Government and Security of Information.” in Information & Security, vol.15, no.1, 2004.

[2]. M. Wimmer & B. Bredow, “A Holistic Approach for Providing Security Solutions in e-government.” IEEE Computer Society, 2002.

[3]. M. Whitman and H. Mattord, , Readings and Cases in the Management of Information Security, Thomson, 2006.

[4]. Security e-Government Strategy Framework Policy and Guidelines, retrieved from: http://www.govtalk.gov.uk/documents/securityv4.pdf

[5]. C. Kalloniatis et al., Security Requirements Engineering for e-Government Applications: Analysis of Current Frameworks, Springer Berlin, 2004.