Model Based Threat and Vulnerability Analysis of E-Governance Systems

Shilpi Saha[1], Debnath Bhattacharyya[2], Tai-hoon Kim[2,*], and
Samir Kumar Bandyopadhyay[3]
[1]*Computer Science and Engineering Department,*
Heritage Institute of Technology,
Kolkata-700107, India
shilpisaha@gmail.com

[2]*Department of Multimedia,*
Hannam University,
Daejeon – 306791, Korea
debnathb@gmail.com, taihoonn@empal.com

[3]*Department of Computer Science and Engineering,*
University of Calcutta,
Kolkata-700009, India.
skb1@vsnl.com

Abstract

The strategic and contemporary importance of e-governance has been recognized across the world. In India too, various ministries of Govt. of India and State Governments have taken e-governance initiatives to provide e-services to citizens and the business they serve. To achieve the mission objectives, and make such e-governance initiatives successful it would be necessary to improve the trust and confidence of the stakeholders. It is assumed that the delivery of government services will share the same public network information that is being used in the community at large. In particular, the Internet will be the principal means by which public access to government and government services will be achieved. To provide the security measures main aim is to identify all possible threats and vulnerabilities according to the data locations and then according to the models of Nath's approach. Based on this analysis, the security requirements of the data and the applications have been formulated in the form of security parameters like confidentiality, integrity and availability. This analysis leads to the security architecture of the specific G2C application.

Keywords: *G2C, Broadcasting model, Critical flow model, Comparative analysis model, E-advocacy model, Interactive model, confidentiality, integrity, availability, authentication, non-repudiation, egovernance*

1. Introduction

Using Information Communication Technology, e-governance is approaching the citizens to provide them web-based services at lower cost and higher efficiency. Among the various components of e-governance, using G2C the citizen can directly interact with Govt. Citizens will be reluctant to use the web based services offered by the government, due to their poor skill, lack of confidence, security and privacy concerns [Backus 2001]. Many of the citizens of the developing countries like India are illiterate. Also, presently there is a lack of

*Corresponding Author

inexpensive and easy-to-use security infrastructure in G2C applications. Moreover, to support all levels of the society, there must be a proper access control technology. Applications security issues like authenticity, confidentiality, integrity, non-repudiation, accountability, etc. need also to be addressed.

In our previous paper [5], G2C applications are classified based on the Egov models. The information flow follows the work flow in these models. The information provided to the citizens is to be reliable, but the information channels are almost always public and insecure. Moreover, there is a necessity for maintaining a secure environment for hosting the govt's data.

This paper looks at the security of the data and systems of G2C applications. Based on this analysis, the security requirements of the data and the applications have been formulated in the form of security parameters like confidentiality, integrity and availability as well the access requirements of the roles. This analysis leads to the security architecture of the specific G2C application.

2. Various Information Security Threats and Vulnerabilities

Examining the overall process, beginning with the consumer and ending with the e-governance server can study e-governance security requirements [Mazumdar 2008]. The assets that must be protected to ensure secure E-governance include client computers, the messages traveling on the communication channel, and the Web and egovernance servers – including any hardware attached to the servers.

2.1 Client End Threats

Until the introduction of executable Web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. But, the widespread use of active content has changed this perception.

2.2. Communication Channel Threats:

The Internet serves as the electronic chain linking a consumer (client) to the egovernance server. Messages on the Internet travel a random path from a source node to a destination node. It is impossible to guarantee that every computer on the Internet through which messages pass is safe, secure, and non-hostile.

2.3. Server end Threats:

The server is the third link in the client-Internet-server trio embodying the E-governance path between the citizen and the government. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

3. Previous work

Based on different classes of information, their sources and frequency of updation and exchange, various models of E-governance projects can be evolved. The National E-governance Action Plan of the Government of India [NeGP] can act as a model for such projects. Other sources of information include and DigitalGovernance.org web page of Mr.

Vikas Nath [Nath, 2005]. In the latter, Nath has classified the models into the following categories:

- Broadcasting / Wider-Dissemination Model
- Critical Flow Model
- Comparative Analysis Model
- E-Advocacy/ Lobbying and Pressure Group Model
- Interactive- Service Model

3.1. Broadcasting Model

The model is based on broadcasting or dissemination of useful governance information which already exists in the public domain into the wider public domain through the use of ICT and convergent media. The utility of this model is that a more informed citizenry is better able to benefit from governance related services that are available for them.

3.2. Critical Flow Model

The model is based on broadcasting or dissemination information of 'critical' value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICT and convergent media. Targeted audience may include media, opposition parties, judicial bench, independent investigators or the wider public domain itself.

3.3. Comparative Analysis Model

Comparative Knowledge Model is one of the least-used but a highly significant model for developing country which is now gradually gaining acceptance. The model can be used for empowering people by matching cases of bad governance with those of good governance, and then analyzing the different aspects of bad governance and its impact on the people.

3.4. E-advocacy Model

E-Advocacy / Mobilization and Lobbying Model is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes. The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking.

3.5. Interactive Model

Interactive-Service model is a consolidation of the earlier presented digital governance models and opens up avenues for direct participation of individuals in the governance processes. Fundamentally, ICT have the potential to bring in every individual in a digital network and enable interactive (two-way) flow of information among them.

4. Our Work and Analysis

In this section we will discuss about the possible threats and vulnerabilities for different data locations and separately for different models. Here data are considered for four locations: data in store, data in process, data in transit and data in destination.

4.1. Broadcasting Model

In broadcasting model, generally data are for public use. So main security concern is to maintain the integrity of data. With this data must be available. Keeping in mind about the four locations of data mentioned above, security aspects, threats and vulnerabilities have been discussed in Table 1.

Broadcasting / Wider Disseminating Model

Public Domain → Wider Public Domain

Table 1. Threats & Vulnerabilities of Broadcasting Model.

Data location	Security Aspect	Threats	Vulnerabilities
Data in Store	Integrity	▪ Encryption cracking	▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Corruption / loss or damage of back up media	▪ Inadequate back up facilities ▪ Non adherence to back up policy
	Authentication	▪ Brute force attack	▪ No Password ▪ Minimum length of the password has not been enforced
Data in Process	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Corruption / loss or damage of back up media	▪ Inadequate back up facilities ▪ Non adherence to back up policy
	Authentication	▪ Theft of credentials ▪ Brute force attack	▪ No Password ▪ Minimum length of the password has not been enforced ▪ Password is guessable
	Data validation	▪ Cross-site scripting ▪ Query string manipulation	▪ Using application-only filters for malicious input ▪ Using non-validated input used to generate SQL queries Relying on client side validation
Data in Transit	Integrity	▪ Encryption cracking	▪ Using the same key for a prolonged period of time
	Authentication	▪ Brute force attack	▪ No Password ▪ Minimum length of the

Data location	Security Aspect	Threats	Vulnerabilities
			password has not been enforced ▪ Password is guessable
	Sensitive data	▪ Network eavesdropping	▪ Passing sensitive data in clear text over network
Data in Destination	Integrity	▪ Encryption cracking	▪ Using the same key for a prolonged period of time

4.2. Critical Flow Model

In critical flow model, data must reach to the targeted domain not to all. So confidentiality is great concern here. All possible security aspects, threats and vulnerabilities have been discussed in Table 2.

Critical Flow Model

Critical Domain → Targeted / Wider Domain

Table 2. Threats & Vulnerabilities of Critical Flow Model.

Data location	Security Aspect	Threats	Vulnerabilities
Data in Store	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Availability	▪ System failure (Unavailability of information system)	▪ Absence of back up policy ▪ Inadequate back up facilities
	Authentication	▪ Brute force attack ▪ Impersonation ▪ Inability to identify actual user	▪ No Password ▪ Minimum length of the password has not been enforced

Data location	Security Aspect	Threats	Vulnerabilities
			▪ Password is guessable ▪ Password sharing among the peer user
	Non-Repudiation	▪ Denial of service attacks ▪ Misuse of privileges	▪ Lack of monitoring of services and activities ▪ Inadequacy in contract documentation (service definition, dos & don'ts and other important processes)
Data in Process	Confidentiality	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small
	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy
	Authentication	▪ Brute force attack ▪ Impersonation	▪ Minimum length of the password has not been enforced ▪ Password is guessable ▪ Password sharing among the peer user
	Data validation	▪ Form field manipulation ▪ Cookie manipulation ▪ HTTP header manipulation	▪ Using non-validated input used to generate SQL queries Relying on client side validation ▪ Failing to validate input from all sources including cookies, query string parameters, HTTP headers, databases and network resources
Data in Transit	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time

Data location	**Security Aspect**	**Threats**	**Vulnerabilities**
			▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Authentication	▪ Brute force attack ▪ Impersonation	▪ Minimum length of the password has not been enforced ▪ Password is guessable ▪ Password sharing among the peer user
	Sensitive data	▪ Network eavesdropping	▪ Passing sensitive data in clear text over network
Data in Destination	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Authentication	▪ Impersonation	▪ Minimum length of the password has not been enforced ▪ Password is guessable
	Non-Repudiation	▪ Denial of service attacks ▪ Misuse of privileges	▪ Lack of monitoring of services and activities ▪ Inadequacy in contract documentation (service definition, dos & don’ts and other important processes)

4.3. Comparative Analysis Model

In comparative analysis model, the analysis is done based on old records. So existing data validation is the main issue. All possible security aspects, threats and vulnerabilities have been discussed in Table 3.

Comparative Analysis Model

Private / Public Domain + Public / Private Domain

→ Wider Public Domain

Table 3. Threats & Vulnerabilities of Comparative Analysis Model.

Data location	**Security Aspect**	**Threats**	**Vulnerabilities**
Data in Store	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy ▪ No back up copy kept off-site
	Authentication	▪ Theft of credentials	▪ Use of weak cipher or hash to make password non readable
Data in Process	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy ▪ No back up copy kept off-site
	Authentication	▪ Theft of credentials ▪ Brute force attack	▪ Use of weak cipher or hash to make password non readable

Data location	Security Aspect	Threats	Vulnerabilities
	Data validation	▪ Form field manipulation	▪ Using input file names, URLs or user names for security decisions
Data in Transit	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Authentication	▪ Theft of credentials ▪ Brute force attack	▪ Use of weak cipher or hash to make password non readable
	Sensitive data	▪ Network eavesdropping	▪ Passing sensitive data in clear text over network
Data in Destination	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Authentication	▪ Brute force attack	▪ Minimum length of the password has not been enforced ▪ Password is guessable

4.4. E-advocacy Model

E-advocacy model has come to the aid of the global civil society to impact on global decision making process. Security aspects, threats and possible vulnerabilities for this model have been discussed in Table 4.

Mobilisation and Lobbying Model

Networking Networks for Concerted Action

Table 4. Threats & Vulnerabilities of E-Advocacy Model.

Data location	Security Aspect	Threats	Vulnerabilities
Data in Store	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size

Data location	Security Aspect	Threats	Vulnerabilities
			that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy
	Authentication	▪ Brute force attack ▪ Impersonation ▪ Inability to identify actual user	▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable
Data in Process	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy
	Authentication	▪ Brute force attack ▪ Impersonation ▪ Inability to identify actual user	▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable
	Data validation	▪ Cookie manipulation ▪ HTTP header manipulation	▪ Failing to validate input from all sources including cookies, query string parameters, HTTP headers, databases and network resources
Data in Transit	Integrity	▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time
	Availability	▪ System failure (Unavailability of information system)	▪ Non adherence to back up policy

Data location	Security Aspect	Threats	Vulnerabilities
	Sensitive data	▪ Network eavesdropping ▪ Information disclosure	▪ Storing secrets when it is not needed ▪ Storing secrets in clear text ▪ Passing sensitive data in clear text over network
Data in Destination	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Authentication	▪ Theft of credentials ▪ Inability to identify actual user	▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable

4.5. Interactive Model

In interactive model, information flows in two ways. So security concern is much higher than all other models. All possible threats and vulnerabilities for this model have been discussed in Table 5.

Service Delivery Model

Citizen ⇄ Government

Table 5. Threats & Vulnerabilities of Interactive Service Model.

Data location	Security Aspect	Threats	Vulnerabilities
Data in Store	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner

Data location	**Security Aspect**	**Threats**	**Vulnerabilities**
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Availability	▪ System failure (Unavailability of information system) ▪ Unsuccessful recovery Corruption / loss or damage of back up media	▪ Absence of back up policy ▪ Inadequate back up facilities ▪ Non adherence to back up policy ▪ No back up copy kept off-site
	Authentication	▪ Impersonation ▪ Inability to identify actual user	▪ Password sharing among the peer user ▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable
	Non-Repudiation	▪ Denial of service attacks	▪ Inadequacy in contract documentation (service definition, dos & don’ts and other important processes)
Data in Process	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Availability	▪ System failure (Unavailability of information system)	▪ Absence of back up policy ▪ Inadequate back up

Data location	Security Aspect	Threats	Vulnerabilities
			facilities
	Authentication	▪ Theft of credentials ▪ Brute force attack	▪ Complexity of the password is not enforced ▪ Use of weak cipher or hash to make password non readable
	Non-Repudiation	▪ Misuse of privileges	▪ Lack of monitoring of services and activities
Data in Transit	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Authentication	▪ Theft of credentials	▪ No Password ▪ Complexity of the password is not enforced
	Sensitive data	▪ Network eavesdropping ▪ Information disclosure	▪ Storing secrets when it is not needed ▪ Storing secrets in clear text ▪ Passing sensitive data in clear text over network
Data in Destination	Confidentiality	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small ▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Integrity	▪ Loss of decryption keys ▪ Encryption cracking	▪ Failing to secure encryption keys ▪ Using the wrong algorithm or a key size that is too small

Data location	**Security Aspect**	**Threats**	**Vulnerabilities**
			▪ Using the same key for a prolonged period of time ▪ Distributing keys in an insecure manner
	Authentication	▪ Brute force attack ▪ Inability to identify actual user	▪ Minimum length of the password has not been enforced ▪ Password is guessable ▪ Password sharing among the peer user ▪ Use of weak cipher or hash to make password non readable
	Authentication	▪ Brute force attack ▪ Inability to identify actual user	▪ Minimum length of the password has not been enforced ▪ Password is guessable ▪ Password sharing among the peer user ▪ Use of weak cipher or hash to make password non readable
	Non-Repudiation	▪ Denial of service attacks ▪ Misuse of privileges	▪ Lack of monitoring of services and activities ▪ Inadequacy in contract documentation (service definition, dos & don’ts and other important processes)

The above tables provide the broad requirements of data storage, communication and delivery security for different models of e-governance applications in G2C domain. The degree of the parameters of security requirements are to be identified on a case by case basis. The advantage of this approach is that the security analyst need not study each and every application separately. Rather, once the G2C application is classified into the specific model, the security requirements can be straight away inferred from the above study. The govt. can also make standards of security based on the e-governance models. Thus there will be less human errors and bias.

5. Conclusion

In summary, this paper presents a methodology to formulate the security architecture of the different G2C applications from their identified models. The methodology and the resulting security architectures can be used for the development, upgrade and audit of the G2C applications in a model-driven manner.

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. So access controls for different stakeholders for different data locations have been defined. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. In this paper, major contribution is the security requirement analysis of the overall G2C applications according to the models.

6. References

[1] Ammal, R. Anantalakshmi, "E-Governance Application Life Cycle Management - Issues and Solutions", egovasia 2007.

[2] Backus, M., "E-governance in Developing Countries", International Institute of Communication & Development (IICD), Research Brief No. 1, March, 2001, http://www.ftpiicd.org/files/research/reports/report3.pdf

[3] Mazumdar, Chandan, Kaushik, Anil K, & Banerjee, Parthasarathi, "On Information Security Issues in E-Governance: Developing Country Views", CSDMS journal, 6th July, 2009.

[4] Nath, V., Digital Governance Initiative, www.DigitalGovernance.org

[5] Anil k Kaushik, Chandan Mazumdar, Jaya Bhattacharjee, Shilpi Saha. "Model Driven Security Analysis of Egovernance Systems" in eIndia 2008, November edition. http://www.egovonline.net/Resource/eindia08-full-paper-for-abstract-173.pdf