Security Issue of E-Governance

Pooja Agrawal
Lect. of IT Department
Dr. C.V.R. University
Kargiroad, Bilaspur(C.G.)
pooja_agrawal148@yahoo.com

Vikas Chandra Pandey
Lect. of IT Department
Dr. C.V.R. University
Kargiroad, Bilaspur(C.G.)
Vickichp@gmail.

Suresh Kashyap
Lect. of IT Department
Dr. C.V.R. University
Kargiroad,Bilaspur(C.G)
Suresh.k1718@gmail.com

Minakshi Agrawal
Lect. of IT Department
Dr. C.V.R. University
Kargiroad,Bilaspur(C.G
minakshi.20@gmail.com

***Abstract:* his is the age of information and technology. There are numerous opportunities for organizations to shape the future by providing efficient services and obtaining a competitive advantage for handling products and services. E-governance refers to application of information technology tools in the administration to provide quick and transparency of information of programmes and policies of the governments to its citizens. The adoption of existing information technologies in the government administration requires operative knowledge. E-government is the use of information technology to support government operations, engage citizens, and provide government services. This definition is actually quite broad. It incorporates four key dimensions, which reflect the functions of government itself: E-services, E-democracy, E-commerce.**

E-government services requires government organizations to implement privacy polices and solutions. This is required to protect individuals from others getting access to information while online services try to increase responding to the needs of online government services. This paper underscores the importance of security in e-governance and also discusses the role of IT security in e-governance.

***Keywords:*- e-Government security, Engineering Life Cycle, Indian Computer Emergency Response Team.**

I. INTRODUCTION

The e-Governance application needs to build the trust of citizens in the system.It needs to ensure that the data and transactions of the citizen are secure. The information shared by the citizens should also remain safe and the privacy of the citizen needs to be protected. Whenever a citizen gets into any transaction with a Government. agency, he shells out lot of personal information, which can be misused by the private sector and anti-social elements. Thus, the citizen should be ensured that the information flow would pass through reliable channels and seamless network. Secured ways of transactions for the Government

services are another issue of concern. The identity of citizens requesting services needs to be verified before they access or use the services. Here digital signature will play an important role in delivery of such services. There is an advantage to making informed decisions for selecting information systems that give organizations added-value in providing products or services to its customers or clients. Without the knowledge of the kinds of technology that exists today and the approaches required to ensure successful project implementation, there can be undesirable consequences or bad decisions can result in cumbersome and time consuming application systems.

II. The various security concerns that may be there for an e-Government System are listed as under:

- □Virus Attacks
- □Outside and Inside Attacks
- User Frauds
- □False identity / Impersonation
- □Unauthorized disclosure
- □Theft / Duplication of access token
- □Misinformation and propaganda
- □Failure to recover business information
- Loss or theft of monetary value

Security Threats:

e-Government security requirements can be studied by examining the overall process, beginning with the consumer and ending with the e-Gov server. The assets that must be protected to ensure secure e-Gov include client computers, the messages traveling on the communication channel, and the Web and egov servers – including any hardware attached to the servers.

Client Threats: Until the introduction of executable Web content, Web pages were mainly static. Coded in Hyper Text Markup Language (HTML), static pages could do little more than display content and provide links to related pages with additional information.

Active Content: Active Contents like Java applets, ActiveX controls, JavaScript, and VBScript refer to programmes that are embedded transparently in Web pages and that cause action to occur.

Malicious Codes: Computer viruses, worms and Trojan Horses are examples of malicious code. People are aware but may not be prepared to deal with such adversaries.

Communication Channel Threats: The Internet serves as the electronic chain linking a consumer (client) to the e-Gov server. Messages on the Internet travel randomly 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.

Confidentiality Threats: Confidentiality is the prevention of unauthorised information disclosure. Use of Internet definitely poses confidentiality threats to the messages sent.

Integrity Threats: An integrity threat exists when an unauthorized party can alter a message stream of information.

SEEK DIGITAL LIBRARY

Availability Threats: The purpose of availability threats, also known as delay or denial of service threats, is to disrupt normal computer processing or to deny processing entirely. Slowing any Internet service will detract citizens from using egov services.

Server Threats: The server is the third link in the client-Internet-server trio embodying the e-Gov path between the citizens and the government. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Web Server Threats: Web server software is not inherently high-risk, it has been designed with Web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes.

Database Threats: Besides government information, databases connected to the Web contain critical and private information that could irreparably damage a enterprise or citizen if it were disclosed or altered.

Common Gateway Interface Threats: A Common Gateway Interface (CGI) implements the transfer of information from a Web server to another programme, such as a database programme. Because CGIs are programmes, they present a security threat if misused. Just like Web servers,

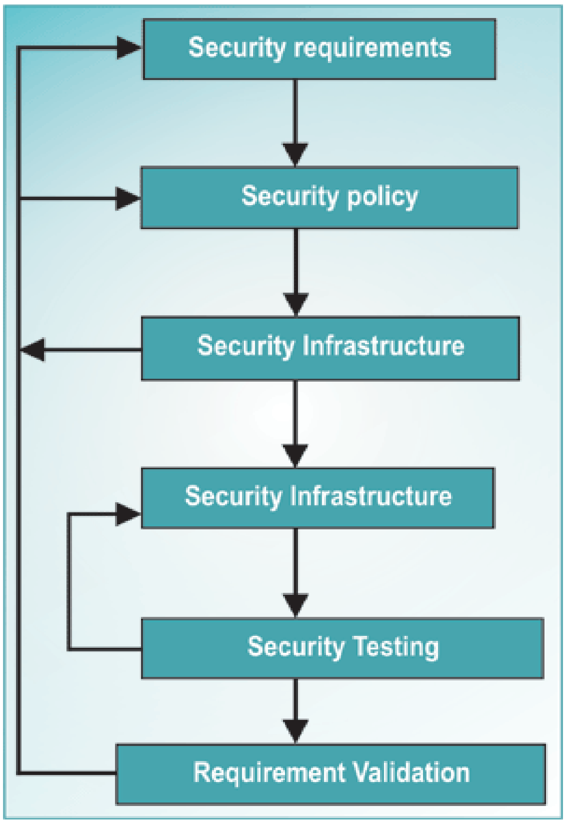

Fig1: Common Gateway Interface Threats

Password Hacking:

Figure:-Security

The simplest attack against a password-based system is to guess passwords. Guessing of passwords require access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

II. A Structured Approach to Security Design:-

Technology components of good online security, such as encrypted email, secure socket layer (SSL) websites, and intranets/extranets all have a role to play in protecting valuable data. For security to be effective it must be designed as a whole and applied consistently across an organisation and its IT infrastructure.

In the case of security systems, the designer has to ensure that the system properties are preserved in the face of attack. The steps to design security of a system is to model the system, identify the security properties to be preserved, model the adversary, and then ensure that the security properties are preserved under attacks. Detailed modeling of the system and identification of the required security properties are possible. But it is almost impossible to accurately model the adversaries and vulnerabilities of the system exploited by those adversaries. The result is that there is nothing called absolute security.

Thus, the system security means: under given assumptions about the system, no attack of a given form will destroy specified properties. Therefore, system security in general and e-Governance security in particular is conceived as a process rather than a one-time developed product.

Security Engineering Life Cycle:-

It is important to note that the e-Governance security need is dynamic rather than static and depends on the operational dynamics. Thereby, the process of designing and deploying an information security infrastructure is a continuous and dynamic process. Often, the change in needs is frequent. In order to be sustainable under such frequent changes, the process has to be developed from a life-cycle approach.

Security Requirement Specification and Risk Analysis: The first phase in the Security Engineering Life Cycle collects information regarding assets of the organisation that needs to be protected, threat perception on those assets, associated access control policies, existing operational infrastructure, connectivity aspects, services required to access the asset and the access control mechanism for the services.

Security Policy Specification: Security Requirement Specification and Risk Analysis Report as input and generates a set of e-Gov security policies. The policy statements are high-level rule-based and generic in nature and thereby, does not provide any insight to system implementation or equipment configuration.

Security Infrastructure Specification: This phase analyses

SEEK DIGITAL LIBRARY

the Security Requirement Specification and the Security Policy Specification to generate a list of security tools that are needed to protect the assets. It also provides views on the location and purpose of the security tools.

Security Infrastructure Implementation: The organisation, in this phase, procures, deploys, and configures the selected security infrastructure at the system level.

Security Testing: In this phase, several tests are carried out to test the effectiveness of the security infrastructure, functionality of the access control mechanism, specified operational context, existence of known vulnerabilities in the infrastructure etc.

Requirement Validation: This phase analyses the extent of fulfillment of the security requirements for implementing e-Governance organization by the corresponding security policy and the implemented security infrastructure. Change in the service goal, operational environment, and technological advancement may lead to a fresh set of security requirements and thereby, triggering a new cycle of the Security Engineering Life Cycle.

III. IT Amendment Act (ITA-2008):-

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In).

The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state.

IV Security area for e-Governance:-

•Dependency on information systems
•High degree of information sharing
•Increase use of remote access
•Challenges of controlling information
•Laws relating to information security
•Dealing with highly sensitive citizen’s and business data
•National security
•Consequences of security breach can be detrimental

V. The importance of security in e-Governance:-

More than most IT systems, e-Governance applications need to be secured. Technology has proliferated in all spheres of life. Accompanied by the rapid growth of the Internet there has been a concomitant rise in online transactions. The government sector has been no exception to these facts and it has wholeheartedly embraced IT in general and Internet-based technologies in particular, of late, in order to extend the benefits of governance to all citizens—urban and rural—through a slew of e-Governance projects. As computer systems have become more user friendly and easy to access, their adoption has grown phenomenally. As a result, we have a scenario wherein multiple operating systems and infrastructure components co-exist. This has increased the potential for security threats.

Security without borders

In the past, guarding the perimeter against external threats was sufficient, but today’s organizations are virtual, global, and dynamic. Simply deploying perimeter-based security is no longer enough to protect data, as information does not reside within static boundaries. On the contrary, a perimeter-centric security model hinders the frictionless movement of information between users spread across the globe what with users accessing data from a variety of devices such as PCs, PDAs, mobile phones, laptops, etc. Attackers and users, both, are not confined to a particular geographical location so it becomes difficult to trace back the attacker. Also users are not always aware of and do not give sufficient importance to security measures. The weakest link in the system is the human one.

Data cannot be confined to one place; the importance of data lies in sharing it. When you share your data, it is spread across several devices including PCs, laptops, data centre servers, mobile phones etc. You need to secure the end-point. Rather than securing the environment, greater emphasis should be given to secure the information that is flowing across several networks.” Information-centric security binds security directly to information and to the people who need it.

The aim of attacks is changing from ‘preserving oneself and wiping out the enemy’ to ‘preserving oneself and controlling the opponent.’ Cyber attacks involve collecting the tactical information and using the same to overpower enemy systems, which brings down servers and thereby, business activities to a standstill.

A full-fledged Cyber attack involves gaining control over networks and there are four steps in it. They are:

1 Gain control over Network of Government and Defense Establishments.
2 Bring down the Financial Systems: The Stock Markets and Banks.
3 Take Control of a Nations’ Utilities (Power, Telecom etc).
4 Take control over personal identities (Passport data / Driving License / PAN No. / Ration Cards etc).

SEEK DIGITAL LIBRARY

Today there are numerous threats—malware, bots, key-loggers, phishing and spoofing to name a few common ones. Lack of security awareness was cited as the biggest cause for attacks.

CERT-In (computer emergency research team-India) along with NIC and other IT vendors has been working towards improving the security levels of IT systems. CERT-In had recently tied up with Quick Heal to deploy the company's anti-virus solution on government PCs.If we can identify the data that we care about and where that data resides, then we need a model to discuss risks and threats.

Draft amendments to the IT Act 2000 lack strong protection against cyber terrorism or cyber war.There should be a combined effort from intelligence agencies, NIC, CERT and the industry to collectively fight a Cyber War." A central nodal agency is required, one that can frame a national strategy for countering insurgency in cyberspace. The creation of national nodal agency for IP Security deployments is vital.

There is a need for security solutions that not only cover security threats from end-to-end but also result in low CAPEX and OPEX. Another important aspect of adopting a security solution is to comply with regulations. Regulations, however, are dynamic and keep on changing. It is to handle this eventuality that the ISO 27001 and ISO 27002 standards had been developed. These adopt a framework approach combining the solutions that are required to cover end-to-end system security. ISO 27001 and ISO 27002 deliver a common language communicating security on a global basis to protect customers, outsourcers, business partners, regulators, auditors and non-security staff.

Furthermore, there is also the need to inculcate security awareness amongst users about recent threats/attacks as well as the dos and don'ts of using Internet. Security has become a key issue that needs to be addressed. Since government deals with sensitive information of national interest, securing data is of utmost importance. The key to securing information, however, does not lie in infrastructure security but the data and information security that are shared over various systems. That is why the need for securing such information has become a priority.

VI. COCLUSION

Information technology has a vital role to play in all transactions that government undertaken. It helps the government cut red tapism, avoid corruption, and reach citizens directly. Such initiatives will help citizens learn about the various policies, process and help lives that government offers. e-Government is a subset of the concepts of Good Governance and SMART Government. It is the very specific task of using the tools offered by security in various aspects of the process of governance with the objective of achieving efficiency, transparency, accountability and user-friendliness in all the transaction s that the citizens and businesses conduct with the Government. Implementation of Security standards are very important for the modernizing Government. Much of e-Governance security involves risk management that is Confidentiality ,Integrity, Availability, Compliance.

ACKNOWLEDGMENT

The authors would like to take this opportunity to thank Vikas Chandra Pandey for his invaluable peer review and editorial work on this article. Her insights were truly appreciated and this paper would not have been possible without her assistance.

REFERENCES

1. [Backus 2001] Backus, M. , "e-Governance in Developing Countries", International Institute of
2. Communication & Development (IICD), Research Brief No. 1, March, 2001.
3. [Bhattacharya, 2003] Bhattacharya, J., "Middleware And Technology Standards For e-Governance", IBM India Research Lab, Research Report, March 2003
4. [Nath, 2005] Nath, V. , Digital Governance Initiative, [PWH 2003] Information Security: A Strategic Guide for Business, ProcewaterhouseCoopers Global Technology Centre, November 2003.
5. [Sengupta, 2005] Sengupta, A., Mazumdar, C. and Barik, M.programmes., "e-Commerce security – A life cycle approach", in Sadhana, Journal of the Indian Academy of Sciences, Bangalore, India, Vol. 30, Part 2 & 3, April/June 2005, Pages 119-140.
6. http://www.bcs-irma.org
7. http://www.itgi.org
8. http://www.bsi-global.com
9. http://www.digitalgovernance.org/.
10. Federal Information Technology Security Assessment Framework
11. Engineering Principles for IT Security –NIST document

SEEK
DIGITAL LIBRARY