Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-254-257
Available online at http://www.bioinfo.in/contents.php?id=55

SECURITY FOR E-GOVERNANCE

ANKUSH JOSHI[1] AND HARIPRIYA TIWARI[2]

[1]Department of Computer Science, Amrapali Institute,Haldwani, Uttarakhand (India).
[2]Department of Computer Science, D.S.B. Campus, Kumaun University, Nainital, Uttarakhand (India).
*Corresponding Author: Email– [1]ankushjoshi1987@gmail.com,[2]haripriya_tiwari87@rediffmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Security is one of the most important issues in E-governance. All of the security approaches that are common in E-commerce are applicable to E-governance. But E-governance is a little different from E-commerce. Usually government networks can communicate to each other better than business networks, because, most of them are connected for transferring information, but businesses are competitors and they don't disclose their sensitive information, so the security of E-government is much more important as compared to E-commerce. Today the users or programmers (Hackers or abusers!) are very smart and intelligent, and they can attack in several forms and so the deffence level has to be sufficiently strong and comprehensive. In this paper we discuss the security of Information and Communication Technology (ICT) system in special relation to E-governance.
Keywords- E-governance, E-commerce, ICT, Security, Threats, DSA, Virtual Private Network, Public Key, Private Key, Virus, Firewalls, IDS, ISMS.

Citation: Ankush Joshi and Haripriya Tiwari (2012) Security for E-Governance. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-254-257.

What is E-governance

When we use various modern information and communication technologies such as Internet, LAN, Mobile's etc. for government to improve the effectiveness, efficiency, service delivery, and to promote democracy then it is called e-governance. We can say E-governance is a system to improve and to support a good government through the use of information and communication technologies. "E-Government is the use of information and communication technologies (ICTs) to improve the activities of public sector organizations[1]". E-governance is a process of delivering information to the user or client in an efficient way for benefit of both client and government.

E-governance is used to provide a SMART government, where SMART captures all the necessary attributes of a good government. In SMART, 'S' denotes 'Simple', 'M' denotes 'Moral', 'A' denotes 'Accountability', 'R' denotes 'Responsiveness' and 'T' used for 'Transparency'.

Security of E-governance

Implementation of E-governance has changed the way of living of the people in various countries. At present scenario we can say our most activities or needs are totally depend upon the E-governance, that's why security of E-governance is a major issue. Here we try to explain an approach for E-governance security which is based on specially two terms i.e. "Security of What?" and other is "Security against What?" in this section we try to work on these two questions.

Security of What?

Security of What? This is a major question when we talk about E-governance security. Security is all about protecting the Information and Communication Technology (ICT) assets of an organization.

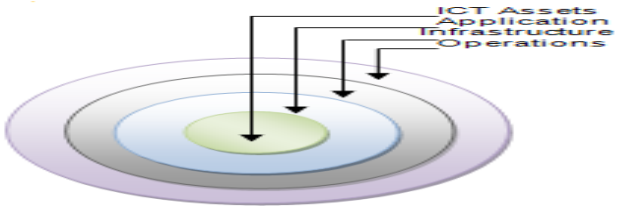

Fig.1- Security Layers

The ICT assets themselves can be of a wide variety including the following:

Data, Information, Knowledge Resources, Programs, Hardware, Networks

Above we mention some ICT assets which are very important for security perspective of E-governance. This is a very important responsibility of E-governance administrators to protect these assets.

Security against What?

There are various threats to security of our ICT system, and we can't define or declare them exactly, it may come from various sources and in various forms. So it is very necessary for e-governance administrator to identify these threats. In this section we firstly give some sources of threats and then some types of threats which affect to E-governance.

Sources of Threat

The sources of threat can be **internal** or it can be **external** to the government body. There are various internal sources of threat like- the employees who work on the E-governance project, customers of the E-governance projects they may attempt to access the databases for their personal financial profit. When we talk about external sources it may be Professional hackers, Criminal organizations, various Intelligence agencies or Investigation agencies.

Types of Threat

Threats may include unauthorized access, modification, and destruction of data. The threats may be of different types varying from time to time because technology changes frequently. The attacks on security of e-governance system can be in different forms including- Defacing of web sites, Hacking, Cracking, Damage to critical database and applications, Network security check list, DSA, Viruses and Malwares etc. the damage of ICT assets need not always be a result of such malicious attacks as mentioned previously. It may be some kind of natural or environmental disasters etc.

Security Management

The above facts lead us to conclusion that the security of the e-governance system has to be managed systematically in three levels, this model is explained with the help of this figure

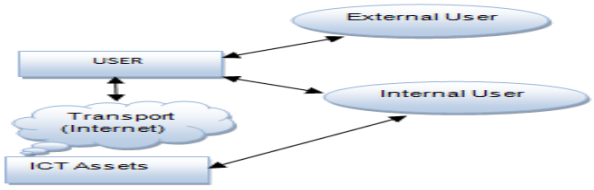

Fig.2- E-governance Security Environment

Security at User Level

Security at user level is a very important issue. We can classify user level security management in three
Parts

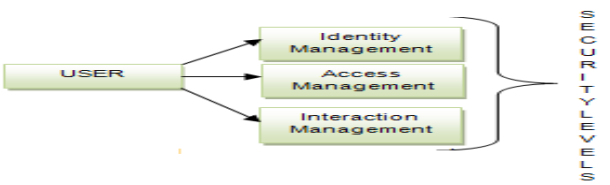

Fig.3-Security at user level

Identity Management

The main purpose of this is to create unique digital identity or credential to all legal users by providing a unique user name and password, to create and manage ICT systems which ensure that the digital identities are secure.

Access Management System

In this level the unique credentials which are provided to the user at identity level are matched to identify the user, that he/she is actually the authentic person.

Interaction Management System

nteraction management is a most comprehensive and complex phase. It includes assurance of the Integrity, Confidentiality and Non-repudiation principles of a comprehensive security.

In user level, we can use various tools such as digital identity token, public key infrastructure (PKI), digital signature, asymmetric key cryptography etc. to provide or enhance the security at the user level.

Security at Transport Level

In this level we consider about e-governance security in two aspects which are security within LAN and WAN, and the second one is Security over the Internet. This security level is classified
into two systems, i.e. Secure Communication System and Cryptographic System.

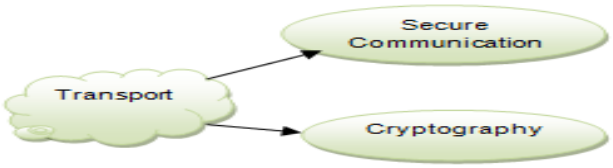

Fig.4- Security at Transport level

The data and information reaches through user to ICT assets or vice-versa, and when the data is in between these two i.e. in transmission medium which can be either LAN, WAN, or any wireless or any other medium whatever, then we need a higher security. For this e-governance administrator use various tools or techniques like creating a Virtual Private Network (VPN), installing Firewalls, using higher and complex Encryption or decryption techniques etc.

Security at ICT Assets level

ICT assets are the most precious for any organization or institution, so to secure this level we have two broad categories of security treatment i.e. Physical security and Electronic security.

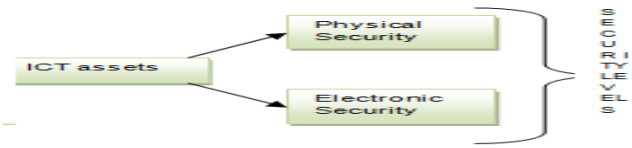

Fig.5- Security for ICT Assets

Physical Security

It is used to protect the data against physical damages or losses like- natural disasters etc. to protect data in this security level we take some steps such as- security level of data centers are highly secured by using biometric-controlled system, in data centers provision of dust-proof environment, fire protection systems, security

alarms, CCTV monitoring of data center etc. automated backup system. By using some basic instructions we easily secure the data physically.

Electronic Security

to give the protection against digital threats we want to use electronic security. We have various electronic security tools, and we can manage them in two categories

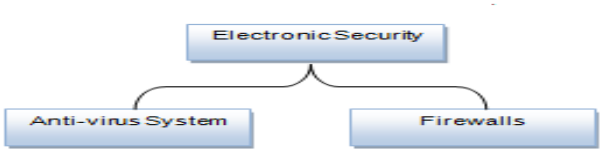

Fig.6- Categories of Electronic Security

Anti-virus System

When we discuss about digital threats the first thing in our mind is virus, which affects our ICT assets in various ways such as- slowing down of the system, occupy disk space, corrupt our valuable data or storage medium etc. it is also known as malware, worms and Trojan horses. there are "over 1,122,311 known viruses active in the world as of 2008[2]".

Firewalls

"A system designed to prevent unauthorized access to or from a private networ[3]". A firewall is a security device that can be hardware or software that is mainly use for to separate a secure area from a less secure area and to control communications between the two. We have several firewall techniques such as Packet filter, Application gateway, Circuit-level gateway, Proxy server. There are many different brands of software firewalls, some of them are- ZoneAlarm, BlackICE and Kerio etc.

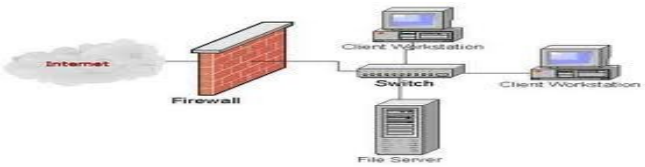

Fig.7- Firewall in an Enterprise

Security Standards-

The standard for information security was set by the BS 7799, being its popularity it was adopted by ISO as ISO 17799 and its sequel BS 7799-2 that prescribes the specification for Information Security Management. "The ISO 27001 standard was published in October 2005, essentially replacing the old BS 7799-2 standard. It is the specification for an Information Security Management System [4]". "ISO 17799 defines 127 security controls structured under 10 major headings to enable the information security manager to identify the particular safeguards that are appropriate to there specific area of responsibility [5]".

Fig.8-Major Security Areas

Security Architecture

The security architecture of E-governance is a high level document that set the security goals of e-governance project and describe the procedure that need to be followed by all the e-governance hierarchy such as users, businesses, operators etc. Appropriate legal framework is absolutely essential for the systematic and sustained growth of e-governance.

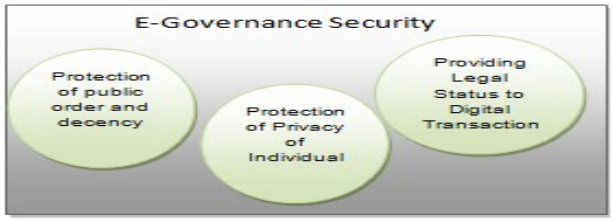

Fig.9- E-governance Security Architecture

Protection of Public Order and Decency

The internet is a highly capable of being saturated and versatile medium at the same time. Its reach is very vast and due to its multimedia capability its impact can be immediate and profound. So the government has to beware of its potential to create a negative impact on society through promotion of terrorism, pornography, communalism, violence etc. Section 67 of the IT Act 2000 of India makes it a punishable offence to "publish or transmit or cause to be published it the electronic form, an material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it [6]".

The enormity of the Internet pornography and immense responsibility of governments in intervention can be gauged from the following statistics on the subject, taken from Internet Filter Review 2004, on 24 October 2003:

- Number of pornographic web sites on the internet: 370 million.
- Number of child pornographic web sites on the Internet:
- 100,000.
- Size of pornographic industry world-wide: US$ 57 billion.
- Size of Internet pornographic industry: US$ 2.5 billion.

Protection of Privacy of Individuals

Disclosure of personal information over the internet raises questions related to the privacy of individuals. The United States passes an Act which is "The Privacy Act of 1974". According to this Act any organization should followed some steps when it gathered any personal information of any individual- Notice, Choice, Onward Transfer and Security

Providing Legal Status to Digital Identities and Transactions-

One of the fundamental requirements of e-governance projects is its ability to create and sustain the operations of government agencies as well as private agencies. So it's very necessary to consult legal status of entities and actions such as- 'legal status is to be provided to the digital identities', 'provide the legal recognition to digital assets', ' provide a digital authority to digital transactions, these transactions could be in the areas of G2G, G2B,G2C etc'. 'Agreements and contracts in digital form'. To providing the authority to any legal digital transaction or deal the Indian government gave 'Information Technology Act 2000' in October 2000. It specifi-

cally takes care of all the issues mentioned above. India followed some provisions of 'Electronic transaction Act 1998 (Singapore)' closely while drafting the IT Act 2000.

Information Security Policy

Information security policy is a document which is prepared by an organization to addresses on the following terms- "why, information security is important for an organization?", "What are the possible security attacks?", "What are the communication channels and ICT assets, which want to protect" etc. that why it is also known as Information Security Management System (ISMS). ISMS is a set of policies which are concerned with security risk's which are related to Information and Communication Technology. "The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks. Furthermore such a company will be capable of successfully addressing information confidentiality, integrity and availability requirements [6]".

Fig.10- Framework of Information Security Policy

Conclusion

As e-governance is the use and involvement of internet and comunication technology to improve different activities of public sector organization, so its security plays a major role as the public's data is flowing in the form of information across different government activities. Through this paper we can know application of different security aspects of e-governance in terms of cryptography issues like user authorization and authentication, non-repudiation and integrity of government issues and many more.

Different govt. activities are being automated with the progressing time but as they are mostly involving common man's information regarding their education, residences, job areas, income and expenditures, involvement in public activities etc. so their security is of major concern. A single leak in the system can deteriorate the full e-governance architecture as all the components are interrelated to one another. So, instead of thinking of security after it has been lost, its better to consider it in advance and have a perfect e-governance system capable of dealing the security aspects as and when faced by it.

References

[1] Prabhudatt Dwivedi and Ganesh P. Sahu *Challenges of E-government Implementation in India*.
[2] *http://www.pcrepairswansea.co.uk/virus.html*.
[3] *www.webopedia.com/TERM/F/firewall.html*.
[4] An Introduction to ISO 27001 (ISO27001).
[5] Satyanarayana J. *e-Government…… the science of the possible*.
[6] The Information technology Act (2000) *The Gazette of India.*
[7] ENISA, Risk management Implementation Principles and Inventories for Risk management / Risk assessment methods and tools. (page 8).