International Journal of Computing and Business Research
(IJCBR)
ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

NETWORK SECURITY SOLUTIONS AND VULNERABILITIES IN E-GOVERNMENT

Mamatha.T[1] and Md.Zair Hussain[2]
Department of Computer Science & Engineering
Maulana Azad College of Engineering & Technology
Patna, Bihar
India

Abstract: Several Indian government websites were hit with denial-of-service attacks by anonymous in May 2012. The rise of e-government has been one of the most striking developments of the web. E-government requires a great deal more than just a solid website that provides the right content. Behind every reliable and efficient application lies an extensive infrastructure of digital networks, application servers and Internet, databases and support services. The citizens expect high standards of services, instant access to information, efficient transactions and support, whenever and wherever they need it but in a secure fashion. Most of the government websites not observing adequate security standards are extremely vulnerable to threats. In this paper we explore two main issues: vulnerability and security in e-government.

Keywords: *E-government, Cryptography, Vulnerability, Security*

1. Introduction

112 Indian government websites were hacked during Dec 2011 to Feb 2012, according to Sachin Pilot, Minister of State for Communications and IT, as reported in India Times. The strategic and contemporary importance of e-governance has been recognized across the world. Basically, one or several web portals supply individuals and businesses with public information, government forms for download, and contact with government representatives. According to most E-Government plans, providing services over the Internet will yield higher efficiency and quality, easier access, the possibility of offering individual services, and increased transparency, ultimately leading to a more efficient public sector. As a result, there are increasing concerns about the reliability and security of the developed websites and applications, in order to ensure that services will be provided to customers with the maximum possible security, to guarantee the integrity of the system and the privacy of online users. The citizens expect high standards of services, instant access to information, efficient transactions and support, whenever and wherever they need it, but in a secure fashion. In this paper our concentration is of security and vulnerability issues in e-government. We propose a strategy to mitigate this risk. Then, conclude a guideline to protect the e-government from these factors and protection from vulnerability as a consequence.

[1]Assistant Professor, Email:mamta.macet@gmail.com
[2]Assoc.Professor & H.O.D, Email:mdzairhussain@gmail.com

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166

Volume 3 Issue 3 September 2012

1.1 E-Government/E-Governance

The term e-government refers to the delivery of government information and services via the web, email or other digital sources.

IT based e-governance projects started with the delivery of e-Seva and Bhoomi successfully. In the next six to ten years, the e-governance will continue to make advances in the use of computers in the government offices for data sharing. Citizens will have more opportunity to interact with the government organizations electronically to download forms, filing reports, bill collections, land registration, online services etc(Figure1). Information technology is used between G2G, G2C and G2B (Figure2).

For data sharing and communication we have end-to-end solutions covering analog, ISDN and leased lines, matching the infrastructure at village or Panchayat offices; routers and leased line modems provide reliable high speed dedicated links between District Offices and State Head Quarters.

The citizens expect high standards of services, instant access to information, efficient transactions and support, whenever and wherever they need it, but in a secure fashion. Our concentration here is security and vulnerability issues in e-government. But first let us take a comprehensive look of vulnerability.

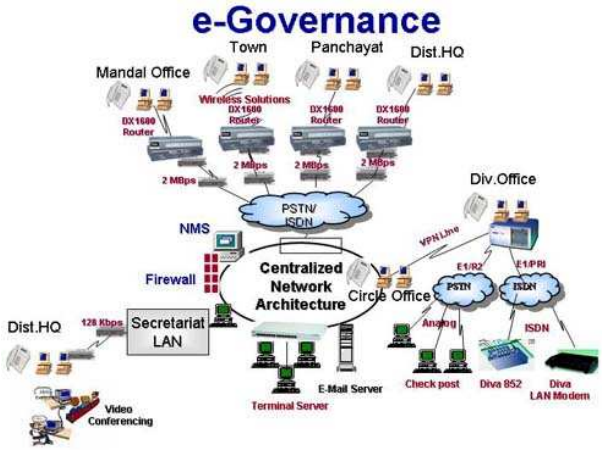

Figure 1: E-Governance Centralized Network

2. Vulnerabilities

Vulnerability may be defined as a feature or bug in a system or a program which enables an attacker to bypass security measures. For any system, there are four regions that can be attacked: peripherals, programs, input and output, and communications. The general factors that affect on the vulnerability in any system are:

2.1 Technical and Technological factors: Technology offers us an incredible number of security tools, like: when a user wants to login to PC, must write the user name and the password, by using encryption and decryption tools, use of Security File System as network file system designed to span the Internet, firewalls, anti viruses programs, PKI systems, and VPNs all these facilities of protecting the systems against the vulnerabilities.

2.2 Human factors: Human factors have several contributions in the vulnerability of the systems- simple configuration mistakes can leave the network ports open, so the firewalls become vulnerable connecting misconfigured systems to the Internet.

2.3 Social factors: The society must have a comprehensive understanding of the security requirements for the systems and applications. Until now, there is gap between the people in the society, some of them have skills to use and understand the computerized systems, on the opposite side, and others don't know anything about it.

2.4 Political factors: By sending viruses, or hacking the passwords or personalized identification of the systems and use it in the competition.

2.5 Economic factors: Usually related with the natural tendency of the society to prefer using an economical solution with short-term benefit. The economic system no necessities to be more secure, it can be less secure and opened to the vulnerability. For example RSA encipherment is better, but DES is widely used because of its quickness.

2.6 Networking factors: Some problems that weaken the security in the telecommunication systems, mistransmissions, interferences, and espionage. Networking problems are crucial to the low quality of telecommunication systems. More than 80% of the e-governments in the world are vulnerable to common web-application attacks such as Cross Site Scripting and Structured Query Language (SQL) injection.

3. Information Security Requirements

These needs are governed by the necessity to protect the following security attributes:

Authentication- This is the ability to say that an electronic communication, whether via email or web, does genuinely come from who it purports to. Forging the "From" field in an email header is a trivial matter, and far more sophisticated attacks are standard fare for hackers. The challenge here is to have simple, cost effective but strong enough authentication method. At least two levels of authentication are recommended.

Privacy- Privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved by enforcing strong security controls in the server systems and via encryption.

Authorization- Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. Authorization is tied with Authentication. If a system can securely verify that a request for information (such as a web page) or a service (purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed. However, in case of e-Governance, the huge and varied type of clientele poses a challenge for the authorization process (Figure 1, Figure 2).

Integrity- Integrity of information means ensuring that a communication received has not been altered or tampered with. Integrity of messages can be achieved in G2B and G2G applications by using digital certificates. However, for general population this will remain a challenge (Figure2).

Non-Repudiation: Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Proper mechanisms and protocols are to be framed for ensuring non-repudiation.

4. Information Security Threats

Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. A cyber attack [2] may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised.

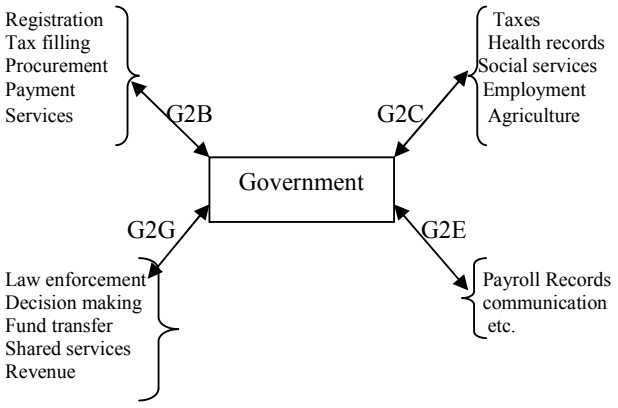

Figure2: E-governance: Structure and Enablers

A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further. Though, it is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he or she can do on the Internet, a college student who has created a new software tool, an

individual seeking personal gain, or a paid "spy" seeking information for the economic advantage of a corporation or foreign country. An incident may also be caused by a disgruntled former employee or a consultant who gained network information while working with a company. An intruder may seek entertainment, intellectual challenge, a sense of power, political attention, or financial gain. Thus, the networks providing data to the end users of the e-Government remain vulnerable to variety of threats such as packet sniffing, probing etc. Table 1 lists some possible threat sources.

4.1 Packet Sniffer- A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. An unauthorized packet sniffing, however, can lead to serious breaches in electronic business and secured transmission.

4.2 Probe- Probe is a class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit e.g. ipsweep, portsweep, nmap, satan.

4.3 Malware- Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior [3]. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code [4]. Malware is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malware includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

4.4 Internet infrastructure attacks- Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

4.5 Denial of Service (DOS) attack- A denial of service attack is a class of attacks where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine e.g. neptune, teardrop, smurf, pod, back, land. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. Exploitation of Trust Computers on networks often has trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

4.6 Remote to Local (R2L) attack- A remote to local attack is class of attacks where an attacker sends packets to a machine over network, then exploits the machine's vulnerability to illegally gain local access to a machine e.g. guss_passwd, ftp,write, multihop, imap, phf, spy, ware master, ware client. An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges. An account compromise might expose the victim to serious data loss, data theft, or theft of services.

4.7 User to root (U2R) attack- User to root (U2R) attacks are a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system e.g. load module, Perl, buffer, overflow, root kit. A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "super user"\ privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs; change how the system works, and hide traces of their intrusion.

Threat	Possible Source
Intentional Threats	terrorists people who dissatisfied with the organization, or has a mental imbalance criminals insiders who colluding with alien enemies
Unintentional Threats	hackers mis-operations from system users
	mis-operations from system chargers or protectors

Natural Threats	earthquake volcanic eruption hurricane flood thunder and lightning hail

Table 1: Possible Threat Sources

5. Improving Security in E-Governance

To make information available to those who need it and who can be trusted with it, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance. It is helpful to begin a security improvement program by determining the current state of security at the site. Methods for making this determination in a reliable way are becoming available. Integral to a security program are documented policies and procedures, and technology that support their implementation.

5.1 Security policy

If it is important to be secure, then it is important to be sure. All of the security policy is enforced by mechanisms that are strong enough. There are organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as information systems, policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology; specific issues:

• Definition of acceptable use for users

• Guidelines for reacting to a site compromise.

• High-level description of die technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy

• Risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss

• Guidelines for system administrators on how to manage systems

5.2 Security Practices

The daily barrage of spam, now infested with zero-day malware attacks, not to mention the risks of malicious insiders, infected laptops coming and going behind the packet-inspecting firewalls and cyber

attacks-prevention systems is the fact of networked communication today. This establishes need for steps of due care and due diligence towards a regulatory compliance, which must be put in place for smooth operations, if not in existence already. System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

• Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.

• Use tools such as MD5 checksums, a strong cryptographic technique, to ensure the integrity of system software on a regular basis.

• Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.

• Be vigilant in network use and configuration, making changes as vulnerabilities become known.

• Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches. Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.

• Audit systems and networks, and regularly check logs.

Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing a cyber attack is difficult. For example, encryption is a best practice and not a product or tool. There are many commercially and freely available tools which may prove to be most suited for a best-practice model.

5.3 Security Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

6. Security Technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect Security.

6.1 Operational Technology

Intruders actively seek ways to access networks and hosts. Armed with knowledge about specific vulnerabilities, social engineering techniques, and tools to automate information gathering and systems infiltration, intruders can often gain entry into systems with disconcerting ease. System administrators

face the dilemma of maximizing the availability of system services to valid users while minimizing the susceptibility of complex network infrastructures to attack. Unfortunately, services often depend on the same characteristics of systems and network protocols that make them susceptible to compromise by intruders. In response, technologies have evolved to reduce the impact of such threats. No single technology addresses all the problems. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

6.2 One-Time Passwords

Intruders often install packet sniffers to capture passwords as they traverse networks during remote log in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected. One common example occurs in remote dial-up connections. Remote users, such as those traveling on business, dial in to their organization's modem pool to access network and data resources. To identify and authenticate themselves to the dial-up server, they must enter a user ID and password. Because this initial exchange between the user and server may be monitored by intruders, it is essential that the passwords arc not reusable. In other words, intruders should not be able to gain access by masquerading as a legitimate user using a password they have captured.

6.3 Cryptography

Sometimes it becomes necessary to encrypt the message sent, with the goal of preventing any one who is eavesdropping on the channel from being able to read the contents of the messages. One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. As millions of electronic messages that traverse the Internet each day, it is easy to see how a well placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture. Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds. The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender first encrypts the information to

protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key. To protect against the chance of intruders modifying or forging the information in transit, digital signatures are formed by encrypting a combination of a checksum of the information and the author's unique private key. A side effect of such authentication is the concept of non-repudiation. A person who places their cryptographic digital signature on an electronic document cannot later claim that they did not sign it, since in theory they are the only one who could have created the correct signature.

6.4 Firewall

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Its purpose is to eliminate from the stream those packets or requests that fail to meet the security criteria established by the organization. A simple firewall may consist of a filtering router, configured to discard packets that arrive from unauthorized addresses or that represent attempts to connect to unauthorized service ports. More sophisticated implementations may include bastion hosts, on which proxy mechanisms operate on behalf of services. These mechanisms authenticate requests, verify their form and content, and relay approved service requests to the appropriate service hosts. Because firewalls are typically the first line of defense against intruders, their configuration must be carefully implemented and tested before connections are established between internal networks and the Internet.

6.5 Analysis tools

There is strong need for analysis tool because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A variety of vulnerability identification tools are available, which have garnered both praise and criticism. System administrators find these tools useful in identifying weaknesses in their systems. Critics argue that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

6.6 Monitoring tools

Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and

examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt. Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis. Understanding of security issues and developing a security perception based on perceived threat profile is important to articulation of a security policy. To translate policy in to a program of action and development of security infrastructure in line with the development of overall IT infrastructure has to be an integral part of e-governance enterprise architecture. The issues underlined and cost benefit tradeoffs have to be analyzed while proposing and implementing a solution.

7. How can we Deploy Vulnerabilities Assessment Successfully

With the expansion of e-governance, the threat and vulnerability to cyber attack on IT assets has increased. A cyber attack can lead to various important services inaccessible to citizens. Also the network and the websites may be corrupted by potential hackers. A total of 112 government websites in India were hacked from December to February 2012. Vulnerability Management is just one type of security control we need.

Protecting networks, systems, data, and applications from threats:

Network security – protection of systems and applications and data begins with good perimeter and network security, which focuses on strategies and technologies to protect enterprises' network and IT infrastructure from external and internal attacks.

Network access control (NAC) – the worm attacks of recent years created demand for a NAC process that would prevent corrupted and dangerous systems from gaining network access. NAC efforts improve defenses against corrupt and dangerous systems by interrogating a node as soon as it is plugged in.

Vulnerability management (VM) – VM focuses on operational processes and technologies needed to discover and remediate security weaknesses before they are exploited. Technologies include VA, security configuration management, patch management, and security event management.

Data protection – focusing on technologies and strategies to protect information where it is stored and as it is used. High-profile data loss events continue to occur with significant financial fraud reported.

Secure messaging and web content – content inspection, compliance, and retention policies cut across all media. Email is one of the most important and visible enterprise security pain points because of threats

such as spam, viruses, spyware, and phishing. Regulations are driving the requirements for improved outbound scanning and encryption.

Application protection – Financially motivated attacks are increasing at the application level as more applications are exposed directly to the Web internally or externally. Applications frequently fail because they have not been built with security in mind.

Mobile security – the majority of mobile and remote user devices, including home PCs, notebooks, PDAs, and smart phones, are not adequately protected. User-owned equipment and mass storage capabilities have only made the situation worse. Many of the largest data breaches have involved the loss of mobile devices containing customer data.

Endpoint security – desktop antivirus products are the largest enterprise security market segment. Growing ineffective antivirus technologies are being augmented by proactive host-based intrusion prevention systems.

Virtualization and virtualized security – this offers opportunities to reduce costs and increase agility and new ways to package security. But it also presents new security threats. Traditional ways of securing physical servers aren't adequate for virtual machines but either it can be deployed successfully as:

Step 1	→	Step 2	→	Step 3
proper planning		careful deployment		detailed follow through

8. Risk Management Countermeasures

Considering the importance of the security of e-government, it is urgent to dispose a whole set of effective countermeasures. The purpose of disposing the countermeasures is to reduce the potential risks and security bugs, so that we can reduce the risk which the e-government system environment facing. Among the e-government risk management countermeasures, it is popular to use defense-in-depth strategy at present. Defense-in-depth strategy, exactly, is consisted of depth security and multi-level security. Through disposing multi-level security protection, we can guarantee that if one level got broken, other levels can still ensure the security of e-government system resources. For example, in case that the outer firewall of one unit got destroyed, by virtue of the inner firewall, the invader still cannot get access to the sensitive data, neither commit any damage to them. Ideally, each level supplies different measures in order to avoid that the hackers can attack different levels in the same way. We have put forward an effective defense-in-depth strategy which is shown in figure 3.

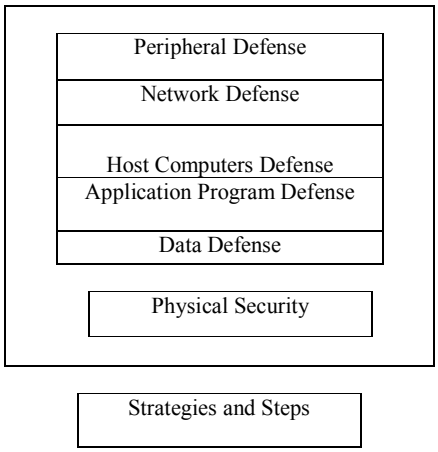

Figure 3: An Effective Defense-in-Depth Strategy

9. Golden Rule for Secure E-Governance

There are no golden rules for risk management. For e-government security risk management, the first step is to scan and detect internal and external environment of the e-government system, check the vulnerabilities and weaknesses of the system. Patch or append new devices immediately in order to reduce the losses as much as possible while risks happen. Secondly, do a full analysis about the e-government security risk, and then make relevant plans and measures. Track and monitor those plans and measures in each implement stage. At last, adjust risk management measures at any time according to the environment changes, and draw up a whole disaster recovery plan.

10. Conclusion

Website security is important and necessary. It is evident from above discussion that for e-governance to be successful, it requires people, process and technology. In Indian e-governance scenario, however, the security aspects are not being taken as seriously. In large number of cases it is not difficult to see that the decision-makers in the government prefer to compromise when it comes to high end technology adoption, implementation and maintenance. Digital security is critical in e-governance initiatives. Confidentiality of any transaction or information available on the network is crucial. The government document and other important material have to be protected from unauthorized users in case of e-governance projects. Hence security is critical for successful implementation of such projects. E-governance coupled with security systems providing adequate protection is the requirement of any system design effort to beat the inertia. We also investigate vulnerability and propose some solution to achieve security.

REFERENCES

Accessed www.msnbc.mns.com for article Anonymous attacks Indian government over file-sharing ban http://www.siliconindia.com/news/technology on 2012-05-10.

Accessed http://www.thetechnologycafe.com/112-indian-government-websites-hacked-in-90-days on 2012-05-10.

Amer N. Abu Ali, Alaa K. Alnaimat and Haifa Y. Abu- Addose, 2010. Evaluating the vulnerability and the Security of Public Organizations Websites in Jordan. Journal of Applied Sciences, 10: 2447-2453.

Mazieres David, Kaminsky Michael, Kaashoek M. Frans,Witchel Emmet, Separating key management from file system security, 17th ACM SOSP , December 1999.

E-government in India: Opportunities and challenges, JOAAG, Vol.3

Defining Malware: FAQ".technet.microsoft.com.http://technet.micros oft.com/en-us/library/dd632948.aspx. Retrieved 2012-02-03.

Cho, Dong-ki. The information society and privacy, media and culture in the information age, Seoul, 1998.

Clarkke, R. A hidden challenge to the regulation of data surveillance, Journal of Law and Information Science 4(2), 1993. No. 2, 2008.

Accessed from www.epaper.techbarrack.com on 2012-04-08