Information Security Measurement and E-Governance

Subhash Chander[1] and Ashwani Kush[2]

[1] Govt PG College Karnal, India
subashjaglan@gmail.com
[2] University College Kurukshetra University, India
akush@kuk.ac.in

Abstract. Security is a buzzword these days. One can hear certain fraud mails, transfer orders, money transfer from bank accounts and many more. Websites are hacked and day by day number of such cases is increasing in whole world. On the other side the number of websites is increasing with huge speed. All the departments whether Government or Private are trying to be online and are in a hurry to provide their more and more services on a mouse click. In such an environment to maintain security of online and digital information is a typical but an important issue. This issue is taken up in this paper and various ways to keep your network/information/website secure are also being discussed. Various existing security metrics their use and hurdles are discussed in the paper. A vulnerability grading scheme has been proposed for the use of novice users. In E-Governance and UID based projects security has to play an important role in their success and failure.

Keywords: EPS, UID, CSC, NeGP, ICT.

1 Introduction

E-Governance means the process of decision making and to implement those processes through electronic means. One can say that Governance is the way those having the power use the power. Governance has social, political, economic and other varied dimensions. E-Government refers to the facilitation of delivery of Government services and main focus is on IT. E-Government uses computing and telecommunication technologies to make radical changes to deliver Government services to its citizens. The major characteristics of governance include participation, Rule of law, Transparency, Responsiveness, equity, inclusiveness, effectiveness efficiency and accountability [1]. In current Indian scenario there is pressure on the political systems and administrators by civil society to share information and make decisions transparent. But such a change can only be possible if there is a change in the minds of the political and permanent executives. Corruption, which is anti poverty, anti-national, anti-economic growth is a major problem faced by India. India ranks 69th out of list of 90 corrupt countries in the world and only 45 paisa out of one rupee is lost in the name of the corruption. Corruption has become a social phenomenon in India. IT can revolutionize the concept of Governance and has the

N. Meghanathan et al. (Eds.): CCSIT 2012, Part III, LNICST 86, pp. 151–159, 2012.

potential to reduce corruption, enhance functioning of Government and deliver the services in a transparent manner. One of the strong pillars of E-Governance is confidence of service users. Business users are found beneficial to information system security risk management when they participate in the various parts of System analysis and design within a business process. User participation raises organizational awareness of security risks and controls within business processes, which in turn contributes to more effective security control development and performance [8]. Confidence can be built if there is fool proof security embedded in the system. Hence if the users of a system are well convinced about the security of a system then they would not hesitate in using the system. Windows operating system are most prevalent systems in the any network private or public. Hence windows operating system has always been the major target of hackers. It will be much better here to clarify the difference between security and safety. Commonly security is concerned with logical resources e.g. money and whereas safety is concerned with physical (including but not limited to human) resources. There is a relation between security and safety. Security problems (relative harm) can often lead to safety problems (absolute harm) [6]. A military operation information about a proposed offensive reaching the opposing force in time leads to improved defenses. In the commercial sphere one can guess similar information regarding future products. For measuring the security of an information system there are certain security metrics.

2 Electronic Service Delivery

Government will be able to inform and query its people over electronic networks in near future. But there are many obstacles to it like digital divide and most of the information is still on papers till date. Governments by nature are conservative organizations and are very slow to adapt a change. Government is also thought of as foundation of society. E-Government can be more productive if it is well implemented and managed [1]. The challenges in the implementation are resistance from people who do not wish to change the status quo and public distrust. Success of Governance lies in formation of policies according to need of present situations and conditions keeping in mind the future and efficient implementation of these policies. Today to switch from the category of Developing countries to developed countries it is the need of the hour to exploit the full potential of ICT. It may either be the use of Internet for the society and solving problems or providing online services to common man .After looking at the cost saving advantages of Internet services, Government has started thinking on providing many basic services online and diminishing the digital divide by opening Information Kiosks at village level. Government has also started providing Internet connections / broadband connections at lower rates through various schemes of centre Government. One such scheme being utilized by Government colleges in Higher Education Department of Haryana is NME-ICT. This scheme is of centre Government, which provides 10 or more Broadband Internet Connections at very subsidized rate with unlimited downloading facility. These services must be utilized by all the academic institutions in states. Only 25% of the cost is to be borne

out by the institution and rest by the centre or state Governments. In a way Government is trying to provide broadband Internet Facility at very low rates so that every common man can take benefit of this electronic world. Infrastructure setup is also being increased by investing a huge amount in purchase of IT apparatus, ensuring electricity and launching satellites in space .Under National E-Governance Plan (NeGP) of Centre Government one lakh Common Service Centers (CSCs) are to opened in the country. From these CSCs basic services (like birth/death certificate, ration card, Income certificate, caste certificate etc.) will be provided at the doorsteps of people.

3 Security Concerns

'Digital Security' gives birth to digital lifestyle and helps to engage confidently in everyday interactions across all digital devices. Digital security affects all aspects of the digital lifestyle, including computers and the internet, telecommunications, financial transactions, and E-Governance applications and their secure access [3]. Internet security means the protection of one's computer's internet account and files from intrusion by an outside user. Internet users of today are very much familiar with internet security products provided by companies like Symantec (Norton Anti-Virus), avast and McAfee. Software provided by these companies helps us to guard against computer viruses, as well as to provide secure firewalls and protection against spyware. For business and e-commerce security organization like CIS (Centre for Internet Security) exists today and is proof of the importance of maintaining adequate internet security [3]. Till date countries power depend on strength of conventional military units for security but in future a country may also depend on how well trained cyber forensic experts and cyber warfare is. In the global world Cyber attacks are increasing day by day and computers control Critical systems that run Power plants, telecommunication infrastructure, air traffic and many more. Security attacks on banks, stock markets and other financial institutions may have a devastating effect on the economy of any country. Economy is the major contributing factor in the development of any country. In case of cyber war there may be break ins in transportation, control systems, financial systems and other utility services being utilized by citizens (may be e-governance services). By keeping in mind the present attacks like 26/11 and the technology being utilized by the terrorists it is the need of the hour have a cyber security cells at various levels in the country. The persons employed in these cells must be of high caliber IT experts and training on latest tools security must be provided so that in future such incidents may be avoided before happening. China is moving ahead in this and is having a cyber warfare army. The core of the attack is that Chinese Cyber Warfare Experts are regularly scanning and mapping India's official networks [5]. More over there is need of proper and strong cyber laws to handle culprits of cyber hacking. There are so many cases of breach of security and online frauds at national and international level. Latest one such a fraud is Speak Asia Online (which asked online people to invest Rs. 11000 and get Rs. 1000 weekly).Proper and strong cyber laws are essential in such cases.

4 Security Measurement

Metrics are the parameters used to ascertain security in the network. In the present digital environment more and more Government activities are going to be online hence one will have to concentrate on various metrics for security of websites and information. Also various penetration loopholes can be taken into consideration before rolling out any online project whether it is related with transaction of online banking or any E-Governance related project involving financial transaction. For any Electronic Payment System (EPS) the major requirements are that it must be secure, flexible and have computational efficiency (support for micro payment & Per transaction cost should be very less).In the modern era there are many risks regarding security in EPS from many angles. From the customer's side, there is danger of stealing payment credentials and passwords. He may also have to face dishonest merchants or financial service providers and there may also be dispute over quality of service or goods. From merchant's viewpoint there may be dishonest or slow financial service providers, there may be forged payment instruments. In case of offline payments there can be danger of insufficient funds in the customer's account. To improve security in such type of EPS one must protect payment credentials with token or smart cards and check for sufficient funds and abnormal spending patterns. Moreover, in the case of Information Technology and Information System security and risk management there is a lack of metrics for years. Having a clear understanding of risk management, in modern IT Environments, gives an important basis for decision making in this area. Such research is clearly necessary, because businesses need tangible figures when provision of security is concerned, not to mention the importance of these elements when an organization is trying to get on the market with a new business model that is focused particularly on security [7]. There are certain myths about the security metrics. Metrics must be objective and tangible. Metrics must have discrete values. One needs absolute measurements. Metrics are costly. It is also essential to measure process outcomes. There is need to handle with numbers [8, 9].

4.1 Related Work

It is commonly known that something can not be managed if it can not be measured and can not be improved if it can not be managed. It also happens in case of security of information systems. Measurements are based on counting whereas metrics are based on analysis. Measuring IT-security is one of the great challenges in modern IT world. Metrics are normally used by industry to gauge performance and evaluate data in areas such as safety, production, efficiency, cost, profitability, and security. A metric is a system of related measures that facilitates the quantification of some particular characteristic. In simpler terms, a metric is a measurement that is compared to a scale or benchmark to produce a meaningful result [11]. Threats in case of information security may be posed by insiders, hackers or crackers, terrorists, organized crime within the nation or states. Insiders, such as staff members, contractor employees, and vendors, may intentionally or unintentionally, damage, or

make susceptible an information system. With the efforts of international organizations security measurement using metrics has attracted great interest in recent years. In 2004, Security Metrics Consortium (SECMET) was founded to define quantitative security risk metrics for industry, corporate and vendor adoption by top corporate security officials of the sector. The Metrics work group of International Systems Security Engineering Association (ISSEA) has led another standardization effort in this area. This group developed metrics for SSE-CMM (System Security Engineering – Capability Maturity Model). One model used widely for conveying the vulnerability severity is the CVSS (Common Vulnerability Scoring System) [13]. Metrics are central for measuring the cost and effectiveness of complex security systems. Without widely accepted security metrics, separating promising developments from dead-end approaches would be very difficult [15]. Security improvement begins by identifying metrics that measure various aspects of security for the organization. Network vulnerability assessments collect huge amount of data that is utilized by experts to draw conclusions. A multi-objective evolutionary approach to cluster data of security assessments is available [4]. Clusters hold groups of tested devices with similar vulnerabilities to detect hidden patterns. Clusters group devices with similar operating systems, open ports, and vulnerabilities.

4.2 Metrics

Metrics can be an effective tool for security manager to distinguish the effectiveness of various components of organization. Metrics can also help identify the level of risk in not taking a given action, and in that way provide guidance in prioritizing corrective actions [12]. Metrics can also be used to raise the level of security awareness within the organization. With the help of metrics managers can answer to the management questions related to security of enterprise as compared to earlier one, comparison of security (earlier and now) and need for more security measures .It is difficult to address security issues using technology only. There must be a balance between technology and issues related to people behavior [14]. The types of measures that can realistically be obtained, and that can also be useful for performance improvement, depend on the maturity of the organization's information security program and the information network and system's security control implementation [17]ï

4.3 Impeding Factors in Security Metrics

Information security is a complex area which makes it difficult but not impossible to identify useful metrics. There are certain factors that should be taken into account and suggest a practical approach to design and implementation of a system of measuring, reporting and improving information security. Several factors impede progress in security metrics:

(a) Lack of good estimators of system security.
(b) Well-established reliance on subjective, human, qualitative input.
c) Lengthened and delusive means commonly used to obtain measurements.

(d) Dearth of understanding and insight into the composition of security mechanisms [16].While removing all vulnerabilities is usually not practical; leaving vulnerabilities unattended may cause significant damages to critical resources in a networked environment. It is thus critical to understand and measure the likelihood of sophisticated attacks combining multiple vulnerabilities for reaching the attack Goal [10].

5 Proposed Work Scales for Vulnerability Checks

Self standard metrics may be thought upon while releasing new software for security (Network or System). There are various options to choose a user while installing the software and most of these options become the reason for the breach of security later on. It would be much better to have numerical value in respect of higher level of vulnerability. Higher the value more is the chances of breach of security in network or system. It is proposed to provide particular values between 1 & 10. The values above 7 may be thought as critical, which means system would be more vulnerable if this option is selected. Similarly from 5 to 7 shows vulnerability but less than the earlier cases. The values from 3 to 5 are of less importance as compared to earlier ones. Values from 1 to 3 are of mild security breach and may not be of importance. Thus a scale has been designed for the providing information to the users that if one selects this option having higher value, then you would not be more secure. Depending upon the values grades may be assigned as 8-10 with Grade A, 6 -7 Grade B, 4-5 Grade C and 1-3 Grade D. Means A grade highly vulnerable ,B means vulnerable, C means less vulnerable and D means unnoticeable (secured) . Corresponding to scale more details may be provided (if desired by users) regarding levels of Vulnerability and what can be the loss in terms of monetary values or assets value or image value.

The above mentioned scheme can be applied in various areas of information security. Also if one has entered into secure area by providing user name and password (may be your mail account or bank account). A particular message on the basis of the above grades must be displayed at the time of entering into the area and it must be asked to user to logout from this session otherwise it is highly risk area. Many of the times email accounts remain open when another user occupies the system. One can enjoy the facility of sending & receiving mails from your account if you have not logged it out. In similar cases if you have entered in online banking/purchasing and you forget to log it out. One may imagine the quantity of loss it may occur. This job can be done with above mentioned scale. E-mails and banking transactions come under the highly risk areas to enter. Hence one can easily remember by looking at the message to log it out when job is finished. Conclusively the scales may be adopted by various software vendors and its proper awareness among the users is must. This scaling type categorization of services can be fully utilized for many e-governance services also. The information related with the land records of a farmer may be taken as “A” grade Vulnerability. Whereas services regarding birth/death, caste certificates may be taken as “C” grade vulnerability.

6 Ways to Secure Transactions

It is clear that the people who attack the web application development systems are vicious. Once hackers recognize that particular website is impenetrable then they will move on to someone else which appears to be more vulnerable [2]. In case of websites certain ports are kept to be opened compulsorily otherwise site may not work or may not be visible by the users for which it is designed. One of the most challenging aspects of creating a web application development is that the rogue elements can come from within the industry. They know all the tricks of the trade and will be able to run rings around everybody so that they can access your website and do as they please [2].To maintain security, industry has developed technology that can mix up sensitive information, such as your credit card number, so that it can be read only by the merchant you are dealing with and your credit card issuer. This ensures that your payment information cannot be read by anyone else or changed along the way. Always look for the picture of the unbroken key or closed lock in your browser window. Either one indicates that the security is operative. A broken key or any open lock indicates it is not. Look to see if the web address on the page that asks for your credit card information begins with "https:" instead of "http." Some web sites use the words "Secure Sockets Layer (SSL)" or a pop up box that says you are entering a secure area. The new beta version of the well renowned search engine has started to provide both of these options now. Some web merchants allow you to order online and give your credit card information over the phone. While doing this, make a note of the phone number, company, the date and time of your call, and the name of the person who has recorded your credit card number. One may want to create a special password for particularly sensitive sites, such as your home banking site. Always use a different password for purchase orders and for logging in Network or computer. Some web sites may require creating a password for future orders. Don't write down any password near computer where someone could see it or carry it in your purse or billfold. If you record it somewhere, then reverse the order of the characters or transpose some letters or numbers. In this way, someone finding it won't be able to know the true password. Be careful about responding to an e-mail, phone call, fax, or letter from anyone who asks for your password(s), social security number, birth date, bank account, credit card number, mother's maiden name, or other personal information. Sellers and financial institutions never ask you for such information unless you are entering into a transaction with them. Identity thieves make up emails that look remarkably like real issue. You should only give your password and credit card number in a secure connection on a web site, not in ordinary e-mail while purchasing online. One should not open any attachment file whose name ends in ".exe." Clicking on such files can install / activate a computer virus that may affect the working of the computer and damage the information stored on computer you are working with. Also keep on updating your anti virus programs time to time [18].

7 Conclusion and Future Work

Information Technology (IT), hardware and software related with IT industry are integral part of nearly every major global industry. PC penetration has increased a lot in the past years. In any web based project security has always been a top issue. IT has become most robust industries in the world and has become key driver of global economic growth. Growth of a country can also be increased if proper information is given to right people at right time. For that security of online services is must. There is always a necessity of new security metrics for the proper security of our information systems. Certain tips, regarding use of online services available and would be available, have been discussed. Various existing security metrics and their role in security are explained. This type of grading is better because a novice user will easily understand whether right options for the security of the information system are being selected or not . Otherwise the technical language incorporated in the softwares is not easily understandable and user may be trapped in the net of hackers unknowingly. Because various ports of the server are being scanned time to time by the hackers to find one open so that they can easily penetrate into the target system. If such scale is used the users can be easily told not to download & not to select the option having A grade (vulnerability).Certain new metrics regarding information security will be provided in future work of study.

References

1. Vasu, D.: E-Governance in India – A reality. Commonwealth publishers (2005)
2. Security aspects in web application development, http://www.webdevap.com
3. Digital security, http://www.en.wikipedia.org
4. Corral, G., Garcia-Piquer, A., Orriols-Puig, A., Fornells, A., Golobardes, E.: Multiobjective Evolutionary Clustering Approach to Security Vulnerability Assesments. In: Corchado, E., Wu, X., Oja, E., Herrero, Á., Baruque, B. (eds.) HAIS 2009. LNCS(LNAI), vol. 5572, pp. 597–604. Springer, Heidelberg (2009)
5. Gaurav, K.: Cyber warfare-a global threat. International Journal of Information Technology and Knowledge Management 2(1), 119–122 (2009)
6. Burns, A., Mcdermid, J., Dobson, J.: On the Meaning of Safety and Security. The Computer Journal 35(1) (1992)
7. Trček, D.: Security Metrics Foundations for Computer Security. The Computer Journal 53(7) (2010)
8. Spears, J.L., Barki, H.: User participation in information systems Security risk management. MIS Quarterly 34(3), 503–522 (2010)
9. Gary, H.: Seven myths about information security metrics. ISSA Journal (2006)
10. Lingyu, W., Tania, I., Tao, L., Anoop, S., Sushil, J.: An Attack Graph-Based Probabilistic Security Metric, http://users.encs.concordia.ca
11. http://www.dartmouth.edu
12. Payne Shirley, C.: A Guide to Security Metrics. A paper on SANS Security Essentials GSEC Paractical Assignment Version 1.2 e (June 19, 2006)
13. Sree Ram Kumar, T., Alagarsamy, K.: A Stake Holder Based Model for Software Security Metrics. IJCSI International Journal of Computer Science Issues 8(2) (March 2011)

14. Asheri, C.J., Louise, Y., Stewart, K.: Security metrics and evaluation of information systems security, A paper available at http://www.citeseerx.ist.psu.edu
15. Victor, P.V., Iustin, P., Sebastian, N.: Security metrics for enterprise information systems. Journal of Applied Quantitative Methods (JAQM) 1(2), 151–159 (2006)
16. Deepti, J., Kavita, A., Sonia, D.: Developing security metrics for information security measurement system. International Journal of Enterprise Computing and Business Systems 1(2) (July 2011)
17. Datta, S.P., Pranab, B.: Guideline for Performance Measures of Information Security of IT Network and Systems. International Journal of Research and Reviews in Next Generation Networks 1(1) (March 2011)
18. Security: http://safeshopping.org