# SECURITY OPTIMIZATION OF E-GOVERNANCE WEBPAGES

**Subhash Chander***

**Ashwani Kush****

**Sharmila*****

## Abstract:

ICT is being applied in various fields nowadays. Affected fields in this category include education, commerce, health and governance. Due to this effect day by day a number of websites and portals are taking birth. No doubt it is for the benefit of the society and its and its people. But as the number of websites and web application are growing exponentially, security of these is becoming main issue. As soon as more and more services are going to be online the risk of losing that information is increasing due to various security concerns. Not only loosing the information, unauthorized changes made in that information may be more dangerous than loss of the data. In electronic form of providing information, the medium is website or combination of websites named portal. In this paper various issues regarding website and portal security have been discussed and various security related suggestions have been provided for the stakeholders.

***Keywords: SSO, XML, SRP, HTTP, HMAC***

* Govt.P.G.College, Sector – 14 , Karnal.

** University College, K.urukshetra Universit. Kurukshetra.

*** Doon Valley Institute of Education, Karnal (Haryana).

## 1.0 Introduction:

A website is collection of web pages, on particular subject or area, linked together. Web portal [5] is a web site that functions as a point of access to information in the World Wide Web. In the knowledge society online information has a great role to play. Information and services to general public is provided through websites and portals. In the earlier times websites were mostly in html format, with few scripts. But the trend has changed to dynamic pages with the advent of technologies like JSP, ASP, XML and XML based technologies like AJAX and MXML [1]. Various types of portals exist but in this study emphasis is on Government portals which are to be utilised by general public. Very soon services like filing Income tax return, filling up application form involving transaction, banking services , registration of land records will be provided through a web portal. In such circumstances there will be need of security of information available on such portals. More than 90 percent of reported security incidents are the result of exploits against defects in the design or code of the software [2]. Software security is a full lifecycle undertaking in which critical design decisions and trade-offs must be clearly and thoroughly understood. Certain characteristics of portals are to be kept in mind before designing it. Portal must be able to accommodate the increasing number of users and applications. It must have capabilities to perform better while handling a large number of people. It must be able to perform complex authorizations for millions of simultaneous users and reduce network traffic by providing 'single sign on' (SSO) [7] rather than repeated authorizations [3]. Flexibility and interoperability of the web portal are also important issues to be kept in mind while designing a portal. By looking at the advantages of the various e-governance services regarding time, money, reliability utilization of these services can not be ignored. But people may hesitate in utilizing these services because of the security breach incidents published through newspapers, magazines etc. Security has great role in E-Commerce, banking and E-Governance sectors [6].portals provide services to its users as a single entity although service may be related to various departments. A single portal is sufficient for filing income tax return and the same can also be used for applying of renewing of driving license. Also the same portal can be used for filing property tax return, depositing electricity and telephone bills. Having a secure e-Government Portal will reduce the costs for the government in delivering timely information to its citizens. The citizens will also benefit from timely and readily available information as well as a medium

to avail services [4]. Security and forensic personnel need to keep up pace with the latest attack tools and techniques adopted by the attackers [8]. Rest of the paper is organized as follows. Section 2 provides literature survey and section 3 provides proposed work for security and motivation of users. Section 4 presents the security concerns of mobiles and computers with certain solution for mobile security. Finally conclusion of the paper is given in section 5.

## 2.0 related work:

Website security is a broad field, but most websites have common security issues that need to be addressed, regardless of the particular technologies used or functions deployed [11]. A number of attacks against Internet Protocol (IP) are possible although it has number of features which make it robust and flexible protocol [16]. Security awareness is major issue to stress upon for the e-governance services to be used by general public. One of the popular techniques, promoted by Microsoft is 'STRIDE' [12]. It involves identifying the category of threats an application may face. Each alphabet of the acronym is expanded into a threat category meaning 'Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, and Elevation of Privileges'. The risk ranking of these threats could be done by another Microsoft technique called 'DREAD' [12] which means 'Damage potential Reproducibility, Exploitability, Affected users and Discoverability'. All the communication that happens between the browser and the server has to be shielded from man-in-the-middle attacks. Such attack occurs when the attacker intercepts messages sent between you and your recipient. The attacker then changes your message and sends it to the original recipient. Solutions for the man in the middle attacks are cryptography and Hashed Message Authentication Codes (HMACs) [18]. If an attacker alters the message, the recalculation of the HMAC at the recipient fails and the data can be rejected being invalid. If the cost of public-key cryptography is a limitation and the services provided do not need the utmost level of security, then alternative technologies or standards that provide comparable transport level security, like the Secure Remote Password (SRP) [5] are embedded in the browser and all server software hosting the government websites. If XML based technologies are adopted, then technologies like web service security with XML encryption and XML signatures can be used between the browsers and the service providers [4]. User should not be worried about any security in using the E-governances through Portals. The browser technology, the transport technology

and the E-Government Server designers have to make sure that the end user is relieved of any security concerns [4].studies have already shown that measures such as, improving information quality, accuracy and currency and introducing trust mark seals help in generating trust in users, studies have also shown that if trust in e-commerce is broken, then it is particularly difficult to regain [19]. So there is an imperative for e-government to get its security right both in terms of hard technical measures and soft management measures.

## 3.0 proposed work for security and motivation of users:

The following information & security measures can help the users in motivating them and building their confidence to utilize the online available e-governance services.

*(a)Availability of services*: Users must know what is available for them online. What kinds of services are available and what they have to pay for the service. Hence publicity for the use of services must be increased and this can be done through various available tools like mobile phones, SMS, and other social media tools.

*(b)Cost of the services:* Since aim is general citizen and the Government services that should be available to the citizens no profit no loss basis. Because in welfare state it is the duty of the government to provide basic services like Ration card, Birth death certificate free of cost. If the cost of such services is there that must be as minimum as possible.

*(c)Convincing about security of the services* : Even if both the above conditions of availability and cost of services are available then the major point of concern is about the security of data that is being taken from users to avail these services. There must be reliability in the system and that can be ensured if there is a validation check on the input output data produced by the system. Security features must be incorporated at every level of system development life cycle.

*(d)More level wise security features:* More security features can be incorporated in e-governance web portals. Presently 'Aadhar' card is being prepared for each and every citizen of India. Hence the database thus created can be used for providing very highly risk services. When portal is there, information available in the database can be utilized for providing services. All the portal services should be divided into three parts namely general services, risky services and highly risky services. General services may be provided without any major hurdle it must be accepted if

input data/information is provided properly. After matching the input data from user side a message can be sent to the user that his request for the service has been accepted. Secondly, For risky services one may employ strong authentication and validation checks. Such checks may include username, password authentication, or e-mail authentication like certain code may be sent to your email and without filling that code you can not move forward to avail the service. Thirdly in case of Highly risky services in spite of the techniques (used for risky services) one may link user data with the biometric card ' Aadhar' .which is unique and details entered by user availing the service can be easily verified and service may be provided after proper authentication. Highly risky service may be the data related with health, tax filing, land ownership and property ownership etc. once the users are convinced about the foolproof security embedded in the portals, the number of users of such portals would automatically increase.

## 4.0 security concerns for computers and mobiles:

A. Computers:

Application developers should also be very particular about security aspects while coding as there are lot of security threats only due to poor writing of application software code. Since many departments are involved in the process of providing services through portals. Each and every department hosting a website must have its security policy and it should be implemented properly and have provision for the punishment for the particular type of breach of security. Before hosting a portal or website proper security audit by authorized parties must be performed so that neither user nor Government should repent on later stages. Various guidelines have been proposed by National Informatics Centre (NIC) for designing Indian Government websites [9]. Various types of vulnerabilities exist in the websites. SQL injection is related to access of database available on the website in unauthorized way. Through SQL injection, attacker is able to access the database with the help of malicious requests. SQL injection vulnerability is more popular than other vulnerabilities and accounts for about 14 percents of web site-related vulnerabilities [10]. If a remote attacker is able to execute OS level commands on the web server then it is called OS Command Injection vulnerability. Session hijacking attack is also possible in case of poor management of session ID. An attacker could steal the session ID of a legitimate user and gain unauthorized access to the services pretending to be the legitimate user. Cross site scripting,

cross-site request forgery, HTTP header injection, third party mail relay, lack of authorization and authentication are the major vulnerabilities in case of websites [10].These vulnerability exist for the development and design level whereas certain measures need to be taken at operational level. Securing web server, encrypting data while communicating may help to overcome some chances of attacks.

B. Mobile application:

Mobile devices with its own advantages will also be used for availing various e-governance services. Now mobile phone is not just a phone to call and listen it has changed a lot since its inception. It is acquiring the features of the computers and is being used by most of the people for checking mail, checking a balance in bank accounts and for social network sites ( facebook, tweeter, linkden etc.). The new invention of Andriod based Ubislate [13] is available and will be utilized by students and general public to avail the online services available. Security is again a great concern in these circumstances as users are novice users. These may be the users who might not have used computers ever before and they may not take into account the basic security points for handling computers and other electronic devices. Attack on mobiles is similar to attack on computers and easiest targets are web browsers and email clients. In mobiles all facilities and features are not available hence attack surface is small on mobile as there is less code to attack [14]. Two more vulnerabilities SMS and GSM radio exist in Mobiles/ smart phones which are not available in computers. Various cyber laws to combat cyber crimes [15] exist in India.

*Security solutions:* Users of mobile phones may be alerted by the banks and other related stakeholders for breach of security. Users must be aware that in case of lack of security what kind of losses one may have to bear upon. If a mobile supports third party soft wares then certain antivirus must be available. Tata Communications and F-Secure Corporation have tied up to offer mobile phone security services in India through all in one security suite for virus protection and integrated firewall. Mobile Security is the easiest & most efficient way to get the required protection for Businesses, which allows automated distribution of the antivirus updates directly to the mobile device over a secure wireless connection [17]. In mobile security soft wares the features like anti spy ware to protect against spy ware, antivirus, firewall are available. Other features included ( for mobiles security) may be anti theft features, automatic updating of antivirus database in the background without user intervention, automatic scanning of files before

saving, copying or downloading to prevent infection, scanning all files on memory cards automatically.

## 5.0 Conclusion:

Internet usage has increased drastically in the past decade. It is natural for Government agencies to embrace the online infrastructure to deliver content as well as services to their citizens. If the users take care of the rules and regulation framed by hardware and software vendors, it will certainly help in diminishing the online attacks on web portal. There is great need to motivate the users to use the portals safely and should have knowledge about basic terms regarding security and attacks. By providing proper training and awareness to the users, and applying secure technologies to web portals, confidence of users to use online web portals can be increased a lot. Mobile security software may help in providing secured e-governance transactions for novice users and such soft wares must be readily available in all smart phones or other such devices which are capable of using internet.

## REFERNCES:


- Misra Anadi," Quality testing of websites", PC Quest, a cybermedia publication, February (2007)
- Mead Nancy,Mcgraw Gary," A portal for software security", Building security In, IEEE security and privacy, July/August (2005) & available at www.computer.org/secuity
- Available at www.entrust.com/resources/pdf/ Buyer's guide, Web portal security solution, Entrust securing digital identities and information
- Saldhana Anil," Secure E-Government portals", W3C Workshop on e-Government and the Web,18-19 June, 2007
- Available at www.en.wikipedia .org
- Chander S.,Kush A.," Secured websites and Infiormation systems",International Journal of Information science and application,Volume 2, number 2,Pp355-358, (2010)

- Available at www.sapportals.com
- Meghanathan Natarajan, Allam Sumanth Reddy and Moore Loretta A.," Tools And Techniques For Network Forensics", International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009
- www.web.guidelines.gov.in
- Nagayasu Yukinobu, Souma Motokuni, Katsumi Naoto, tokumaru Hiroshi,Takagi Hiromitsu," How to secure your website" Approaches to Improve Web Application and Web Site Security, 4th edition ,June (2010) available at www.ipa.go.jp/security
- "Top 10 website security issues" , available at www.watsonhall.com/methodology/top10s/.pl.
- Kadam Avinash W ," Database and Application Security– Defense in Depth" CSI Communication ,December 2011
- "A beginner guide to network security", available at www.cisco.com/go/security ,
- Miller Charlie,"Mobile Attacks and Defense ", IEEE security and privacy,july 2011
- Mali Prashant," Types of cyber crimes & cyber law in India",CSI communication , November (2011)
- Curtin Matt,"Introduction to network security", March (1997), available at www.interhack.net/pubs/network-security/
- Available at www.newtechnology.co.in
- Available at www.msdn.microsoft.com/en-us/library/s
- Tassabehji Rana," Inclusion in e-government: a security perspective", *e*Government Workshop '05 (*e*GOV05), September 13 2005, Brunel University, UK