International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195198

Anticipated Security Model for Session Transfer and Services Using OTP

J. Jose Merlin[1], A. Prathipa[2], G. Ramyadevi[3], P. Radhika[4]

[1-3]Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Thanjavur, Tamil Nadu, India

[4]Assistant Professor, Department of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Thanjavur, Tamil Nadu, India

ABSTRACT

Internet security is a branch of computer sciences often involving browser security, network security, applications and operating systems to keep the internet as a secure channel to exchange information by reducing the risk and attacks. There are a number of studies that have been conducted in this field resulting in the development of various security models to achieve internet security. However, periodic security reports and previous studies prove that the most secure systems are not immune from risk and much effort is needed to improve internet security. This paper proposed a simple security model to improve internet applications security and services protections, specified access control, cryptographic, cookies and session managements, defense programing practices, care for security from early stage on development life cycle, use hardware authentication techniques in access control, then propose cryptographic approach by mix MD5 with Based64, consider session and cookies types and ways to keep it secure. Additionally, these practices discussed the most important web security vulnerability and access control weakness and how to overcome such weaknesses, proposed an approach to measure, analyze and evaluate security project according to software quality standard ISO 25010 by using Liker scale, finally ended by case study. The effort of this paper represents a set of techniques and tips that should be applied within each web application development process to maintain its security.

Keywords : Combinationarial Optimization Identification, Public Key Infrastructure, Partial Forward Secrecy.

I. INTRODUCTION

Web applications emerged as one of the main technologies and progressed in the last decade. They play a main role in our daily lives on areas such as health-care, online services, businesses (public and private sectors), E-banking, and e-commerce. Web applications are expected to increase the trading volume on the market exceeding $ 1 trillion in the next several years. Many public or private enterprises developed their applications and services based on the internet to take advantage of its features as well as efficiency, simplicity, and cost effectiveness. On the other hand, these enterprises face a new challenge on how to keep these applications and services secure. They are spending many resources to manage and handle data storage in plain text in malt locations throughout the enterprise. Recently, the security of web applications and services derived attention from both the industry field and research community. There is a strong need for standard web security models for several reasons including: the integration of the heterogeneous and distributed systems, availability of high volumes of sensitive

information and data maintained by corporation's servers and government agencies, safety from easily distributed malicious software, and computer crimes. On the other hand, software security has become a quality attribute used to measure the quality of software according to standards such as ISO software quality standard 25010.

II. LITERATURE SURVEY

Proposed Security Model For Web Based Applications And Services

Internet security is a branch of computer sciences often involving browser security, network security, applications and operating systems to keep the internet as a secure channel to exchange information by reducing the risk and attacks. There are a number of studies that have been conducted in this field resulting in the development of various security models to achieve internet security. However, periodic security reports and previous studies prove that the most secure systems are not immune from risk and much effort is needed to improve internet security. This paper proposed a simple security model to improve internet applications security and services protections, specified access control, cryptographic, cookies and session managements, defense programming practices, care for security from early stage on development life cycle, use hardware authentication techniques in access control, then propose cryptographic approach by mix MD5 with Based64, consider session and cookies types and ways to keep it secure. Additionally, these practices discussed the most important web security vulnerability and access control weakness and how to overcome such weaknesses, proposed an approach to measure, analyze and evaluate security project according to software quality standard ISO 25010 by using Likert scale, finally ended by case study. The effort of this paper represents a set of techniques and tips that should be applied within each web application development process to maintain its security.

Security Issues for Web-Based Applications: Issues And Solutions For The Safe Transfer Of Clinical Trials Data Over The Internet When building any web-based application, the issue of security is always a concern. When the application is designed to allow the sharing of clinical trials data across the Internet, security becomes one of the major topics. This paper describes what approach iBiomatics, a SAS company, has taken in the construction of their biometrics Portal. The paper presents a basic overview of security for an Internet based application, describes what security features were built into the application, what software tools were used to implement various aspects of the security model, and how the actual hardware configuration can be a critical piece of the overall security of a web based application.

Securing Frame Communication in Browsers

Many web sites embed third-party content in frames, relying on the browser's security policy to protect them from malicious content. Frames, however, are often insufficient isolation primitives because most browsers let framed content manipulate other frames through navigation. We evaluate existing frame navigation policies and advocate a stricter policy, which we deploy in the open source browsers. In addition to preventing undesirable interactions, the browser's strict isolation policy also hinders communication between cooperating frames. We analyze two techniques for inter-frame communication. The first method, fragment identifier messaging, provides confidentiality without authentication, which we repair using concepts from a well-known network protocol. The second method, post Message, provides authentication, but we discover an attack that breaches confidentiality. We modify the post Message API to provide confidentiality and see our modifications standardized and adopted in browser implementations.

Protecting Browsers From Dns Rebinding Attacks

DNS rebinding attacks subvert the same-origin policy of browsers, converting them into open network proxies. Using DNS rebinding, an attacker can circumvent organizational and personal firewalls, send spam email, and defraud pay-per-click advertisers. We evaluate the cost effectiveness of mounting DNS rebinding attacks, finding that an attacker requires less than $100 to hijack 100,000 IP addresses. We analyze defenses to DNS rebinding attacks, including improvements to the classic "DNS pinning," and recommend changes to browser plug-ins, firewalls, and Web servers. Our defenses have been adopted by plug-in vendors and by a number of open-source firewall implementations.

Assessment of Access Control Systems

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. In some systems, complete access is granted after successful authentication of the user, but most systems require more sophisticated and complex control. In addition to the authentication mechanism (such as a password), access control is concerned with how authorizations are structured. In some cases, authorization may mirror the structure of the organization, while in others it may be based on the sensitivity level of various documents and the clearance level of the user accessing those documents. This publication explains some of the commonly used access control services available in information technology systems.

III. EXISTING PROCESS

Password-based authenticated key exchange is protocols which are designed to be secure even when the secret key or password shared between two users. The main goal of password-based authenticated key exchange protocols is to restrict the adversary to this case only. The existing system consider that password-based authenticated key exchange in the three-party scenario, in which the users trying to establish a secret do not share a password between themselves but only with a trusted server. In this existing system the key exchange between three authenticated users so, that the privacy of the system is failed to overcome. Since we want to trust as little as possible the third party, we develop a new notion called key privacy which roughly means that, even though the server's help is required to establish a session key between two users in the system, the server should not be able to gain any information on the value of that session key.

IV. PROPOSED METHODOLOGY

A secure 2-party password-based key exchange is a 2PAKE protocol where the parties use their password in order to derive a common session key that will be used to build secure channels. Several practical schemes can be used in the instantiation of the 2-party password-based key exchange of our generic construction. In these proposed system, instead of exchange the password the owner going to send the link to get that particular data and in user side by using that link they can retrieve that data easily. Once the user make logout means they cannot again enter into the system. The link can be used only once.

V. IMPLEMENTATION RESULTS

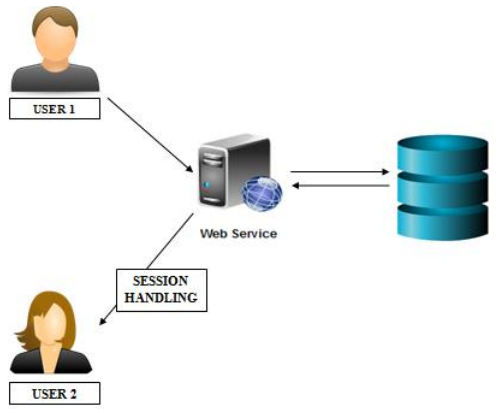
Search engine recognized

Search engine indexing collects, parses, and stores data to facilitate fast and accurate information retrieval. Index design incorporates interdisciplinary concepts from linguistics, cognitive psychology, mathematics, informatics, and computer science. An alternate name for the process in the context

of search engines designed to find web pages on the Internet is web indexing.

Popular engines focus on the full-text indexing of online, natural language documents. Media types such as video and audio and graphics are also searchable.

Meta search engines reuse the indices of other services and do not store a local index, whereas cache-based search engines permanently store the index along with the corpus. Unlike full-text indices, partial-text services restrict the depth indexed to reduce index size. Larger services typically perform indexing at a predetermined time interval due to the required time and processing costs, while agent-based search engines index in real time.



Optimized search results

Search engine optimization (SEO) is the process of affecting the online visibility of a website or a web page in a web search engine's unpaid results—often referred to as "natural", "organic", or "earned" results. In general, the earlier (or higher ranked on the search results page), and more frequently a website appears in the search results list, the more visitors it will receive from the search engine's users; these visitors can then be converted into customers.[1] SEO may target different kinds of search, including image search, video search, academic search,[2] news search, and industry-specific vertical search engines. SEO differs from local search engine optimization in that the latter is focused on optimizing a business' online presence so that its web pages will be displayed by search engines when a user enters a local search for its products or services. The former instead is more focused on national or international searches.

Authentication

An authentication module is a plug-in that collects user information such as a user ID and password, and compares the information against entries in a database. If a user provides information that meets the authentication criteria, the user is validated and, assuming the appropriate policy configuration, granted access to the requested resource. If the user provides information that does not meet the authentication criteria, the user is not validated and denied access to the requested resource. OpenSSO Enterprise is deployed with a number of authentication modules.

Session Handling

A web session is a sequence of network HTTP request and response transactions associated to the same user. Modern and complex web applications require the retaining of information or status about each user for the duration of multiple requests.

User preference

Understanding user preference settings. Completing the user preferences pages enables the system to use the field values that you specify as the default data that appears on various inquiry pages. ... This enables default values to be set by user ID; the user can override the defaults when running an inquiry.

Temporary User Restriction

To ensure a consistent user experience, we monitor the level of requests to the my hr toolkit system from user accounts. If an abnormally high frequency of requests is detected, an escalating blocking process is deployed

VI. CONCLUSION

Thus the process a secure 2-party password-based key exchange is a 2PAKE protocol where the parties use their password in order to derive a common session key that will be used to build secure channels. Several practical schemes can be used in the instantiation of the 2-party password-based key exchange of our generic construction. In these proposed system, instead of exchange the password the owner going to send the link to get that particular data and in user side by using that link they can retrieve that data easily. Once the user makes logout means they cannot again enter into the system. The link can be used only once.

VII. FUTURE ENHANCEMENT

The introduction of VoIP has enabled many organizations to supplement or replace existing circuit switched telephone networks, providing a new value added services. Numerous technological problems are faced on the issue of quality of service. The packet loss is a major problem. This problem cannot be avoided but it can be minimized. The packet repetition with static playout algorithm performs moderately than other replacement techniques. Based on time delay, loss rate and MOS, the better results are obtained. Hence, the receiver based repetition provides high quality VoIP signal in the streaming audio. The processing of damaged packets has been established as a challengeable topic for further research. This work can be extended by incorporating other statistical based methods. Voice over IP provides unique and inexpensive services to the internet people. Internet is a single network shared by the world. Audio conferencing is one of the applications used nowadays in the internet community. This is purely based on multiplexing and multicasting scheme. It promises to deliver cost savings to users and service providers. Hence the Voice M-M based interleaving provides high quality VoIP signal in the streaming audio. This work can be extended by incorporating video based methods. It offers improvements in quality and video conferencing applications in the near future.

VIII. REFERENCES

[1]. Michel Abdalla, Pierre-Alain Fouque, and David Pointcheval, "Password-Based Authenticated Key Exchange in the Three-Party Setting", IEEE Proceedings on InformationSecurity, Volume 153, number 1, March 2006 , pp. 27-39.

[2]. Whitefield Diffie, Martin E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644-654,1976.

[3]. Behrouz A. Forouzan, Cryptography and network security, Tata McGraw-Hill, 2007.

[4]. Hyun-SeokKim ,Jin-Young Choi, "Enhanced passwordbased simple three-party key exchange protocol", Elsevier, Computers and Electrical Engineering, 35, pp.107–114,2009.

[5]. Yuanhui Lin, MengboHou, Qiuliang Xu, "Strongly password based three party authenticated key exchange protocol", Ninth International conference on Computational Intelligence and security, IEEE, pp. 555- 558,2013.

[6]. Rongxing Lu, Zhenfu Cao, "Simple three-party key exchange protocol", Elsevier, computers & security 26, pp. 94-97,2007.

[7]. Chao Lv , MaodeMab, Hui Li, JianfengMaa, Yaoyu Zhang, "An novel three-party authenticated key exchange protocol using one-time key", Elsevier, Journal of Network and Computer Applications (36), pp. 498–503,2013.

[8]. Alfred Menezes, BerkantUstaoglu, "On reusing ephemeral keys in Diffie Hellman key agreement protocol",International Journal of Applied Cryptography,ACM,pp. 154-158, 2010.

Cite this article as : J. Jose Merlin, A. Prathipa, G. Ramyadevi, P. Radhika, "Anticipated Security Model for Session Transfer and Services Using OTP", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 414-418, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT195198
Journal URL : http://ijsrcseit.com/CSEIT195198