Secure Web Based Single Sign-On (SSO) framework using Identity Based Encryption System

Rajesh Kumar Singh
Department of Computer Engineering
National Institute of Technology Karnataka, Surathkal,
INDIA
rajeshsingh.nitk@gmail.com

Alwyn R Pais
Department of Computer Engineering
National Institute of Technology Karnataka, Surathkal,
INDIA
alwyn.pais@gmail.com

Abstract- Due to the vulnerability caused by poor password selection it is very important to have a secure authentication and authorization infrastructure for web based applications. In the current scenario it is very difficult to remember different passwords for different web based applications. We propose centralized password based multiuser and multi-application Single Sign-On (SSO) framework for such applications. Unlike traditional Single Sign-On architectures we are using Identity Based Encryption System (IBES) instead of Public key infrastructure (PKI). Our proposed design provides better security for the users and the system is efficient. This framework is deployed as a web service and can be deployed on a web server.

***Keywords* — IBES, SSO and Security**

I. INTRODUCTION

Authentication is one of the major aspects of cryptography. Password based authentication is a common authentication mechanism used in web based applications. In the increasing use of internet, remembering several logins and passwords is a tedious job, so most of the time people select simple logins and passwords. This easy memorable password makes the system vulnerable to attack.

Single Sign-On provides an authentication and authorization infrastructure that solves the problem created by poor password selection. SSO is a process of authenticate once and gain access of multiple resources. Aim of SSO is to reduce number of login and password in heterogeneous environment.

In this paper, we have designed and implemented a SSO framework with centralized password based authentication mechanism at SSO server and local authentication and authorization at web-based applications. Our design satisfies security requirements for safe storage and exchange of data among different entities.

Rest of the paper is organized as follows. Related work is explained in section II. Section III discusses security requirements. SSO system architecture is given in section IV. Authentication and Authorization process is given in section V. System analysis is done in section VI. Section VII explains the implementation details. Section VIII concludes the paper followed by references.

II. RELATED WORK

Several Single Sign-On frameworks were proposed and implemented so far but they are not balance in Security, Efficiency and Usability.

The systems discussed in [1] and [2] are based on PKI and agents. These systems provide enough security but efficiency and usability are poor. PKI certificate is use to authenticate users. Creation, revocation and distribution of these certificates make the system more complex and inefficient [8].

Cookie based SSO systems [4], [6] suffer from session hijacking i.e. exploitation of valid session. Cookies are sometimes encrypted using same session key, so if the attacker can find the session key for even one cookie, every user cookie is now vulnerable [6].

Our proposed framework uses Identity Based Encryption System [7]. IBES removes complexity involved in PKI based system and improves efficiency of system. We have proposed centralized password based authentication infrastructure and secure way to exchange information among user and different applications. Each Application has its own local password based authentication and authorization.

III. SECURITY REQUIREMENTS

In this section we discuss security requirements that our proposed SSO infrastructure needs to fulfill.

- There should be balance among security level, usability and performance.
- Data leakage should be avoided to protect user's privacy.
- There should be some mechanism to secure exchange of information during authentication and authorization process.
- SSO server should not get any personal information of user by any means.
- Mutual authentication should take place between users and web applications.

978-0-7695-3845-7/09 $26.00 © 2009 IEEE
DOI 10.1109/ARTCom.2009.82

IV. SSO SYSTEM ARCHITECTURE

This section describes secure system architecture for SSO. The SSO system contains four components:

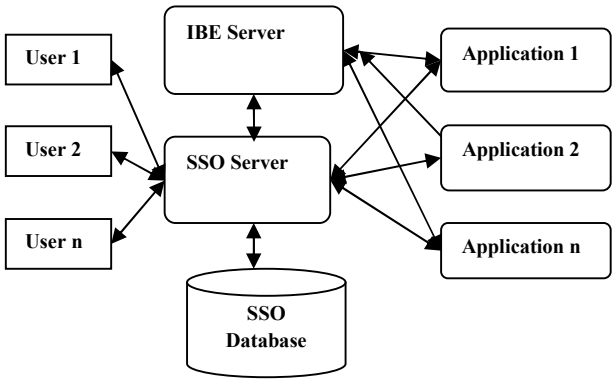

Fig. 2. SSO System Architecture

(1) Client: They are application users. In our framework users need to authenticate themselves in SSO server by login and password.

(2) IBE Server: IBE Server is responsible to generate private key. It takes URL (URL of application or SSO) as input and generates private key.

(3) Applications: They are special purpose web based applications like internet banking, online shopping, email server, etc. Each application has its own password based authentication and authorization process.

(4) SSO Server: This is an intermediate server among users and web based applications. SSO is responsible for authentication of user. Data exchange platform maps login and password of user with credential stored in database.

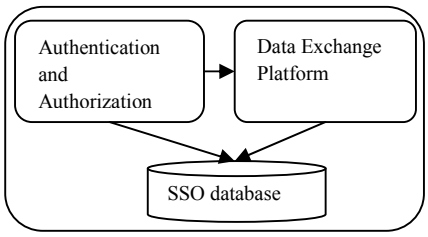

Fig. 4. SSO Server

V. AUTHENTICATION AND AUTHORIZATION PROCESS

This process has three phases: initial setup, profile creation and runtime phase.

A. Initial setup phase

- IBE Server initializes its system parameters and generates master-key.
- SSO server and each web applications have to get their private key from IBE Server (PKG). Before getting private key they have to register in the PKG and create profile.

B. Profile creation phase

- User access SSO server Sign-Up page and creates its profile by selecting its login and password for SSO server. Login is unique in SSO server database.
- After creating profile user can authenticate to SSO server by providing login and password. This login and password is encrypted using URL of SSO server as public key. SSO Server decrypts these by its private key.
- Now user can put authentication and authorization information of different web applications into SSO Servers database. Authentication and authorization information of a particular application is encrypted using URL of that application as public key.

C. Runtime Phase

- User authenticates to SSO server by providing login and password encrypted using URL of SSO as public key.
- User can select application available in the list of SSO server. User can only select the applications where he/she has previously inserted authentication and authorization data.
- This Authentication and authorization data is provided to particular application where these data are decrypted and local authentication is done.
- Now user is connected to application and can access the services provided by that application.

VI. SYSTEM ANALYSIS

Our proposed SSO architecture provides reasonable security without compromising efficiency and usability. IBE system uses elliptic curve cryptography where as PKI uses RSA algorithm as public key cryptography algorithm. As shown in TABLE I, the Elliptic Curve Cryptosystem (ECC) offers the higher strength per bit as compare to RSA algorithm [9].

TABLE I

COMPUTATIONALY EQUIVALENT KEY SIZE

ECC	RSA
163	1024
283	3072
409	7680
571	15360

A. Securing SSO server from possible attacks

In IBE system, there is no public key exchange, nor certificate retrieval or verification, before a message transfer; hence man-in-the-middle attack is not possible. All authentication and authorization data related to particular

application are stored in database of SSO server after encrypting using URL of that application as public key. Even if data is stolen it cannot be decrypted, because decryption key (private key) is with application only. IBE scheme is semantically secure against an adaptive chosen cipher attack [7].

B. *Satisfaction of security requirements*

In this section we will discuss how our system is fulfilling security requirements discussed in section III.

- IBES makes system secure and efficient as compare to PKI. In IBES encryption can be done by any ID like URL, etc, this makes system easy to use.
- Privacy is maintained by encrypting authentication and authorization data using URL of application as public key.
- Exchange of authentication and authorization information is made secure by encrypting it using receiver URL as public key.
- SSO server can not directly map individual user with their authentication and authorization information of different applications. So user's anonymity is guaranteed.
- In runtime phase mutual authentication takes place between user and application.

VII. Implementation and Results

We have developed a SSO server, an IBE server and three small web based applications. All these entities are implemented using java programming language version jdk1.6.0_02. All servers are developed as servlet and JSP in Tomcat5.0 Web Server. Authentication and authorization data is stored in MySQL database.

A. *Server availability*

The availability of the SSO server is tested using the "HTTPattack: An Open Source Web Stress Tool" [10]. The burst of requests are sent to the server running the web application and the number of requests that the server can handle is measured.

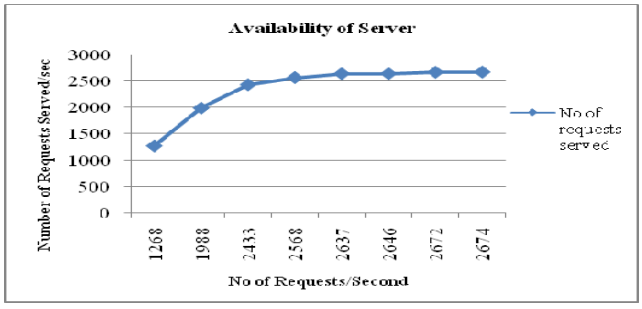

Fig. 5 Availability of the server

B. *Average Response Time*

Fig. 6 Shows Average Response time of SSO server taken at different load conditions.

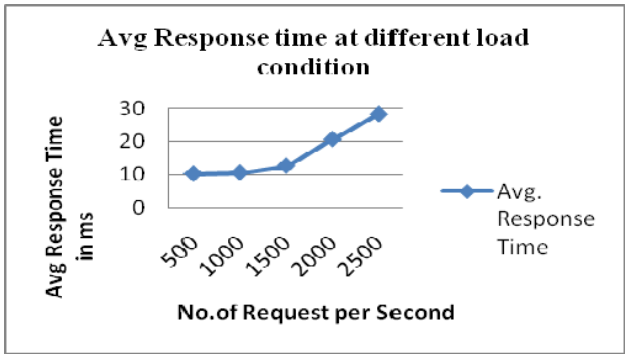

Fig. 6 Average Response Time

VIII. Conclusion

We have proposed novel Web based Single Sign-On System using Identity based encryption system. Proposed system is secure, efficient and usable as compare to traditional PKI and agent based system. All authentication and authorization information is stored in SSO server database in encrypted form. Proposed framework is implemented using java and tested for three different prototype web based applications. Proposed system is vulnerable against man in the middle attack, data stealing and chosen adaptive cipher attack.

References

[1] Kee-Boem Nam and Roan-Sung Kwak "On the Efficient PKI System with SSO" IEEE International Conference on Control, Automation and System 2007, Oct. 17-20, 2007 COEX, Seoul, Korea.

[2] Somchart Fugkeaw, Piyawit Manpanpanich and Sekpon Juntapremjitt "A Robust Single Sign-On Model based on Multi-Agent System and PKI" Proceedings of the Sixth International Conference on Networking (ICN'07) IEEE 2007.

[3] Ye Jun, Li Zhishu, Ma Yanyan "JSON Based Decentralized SSO Security Architecture in E-Commerce" International Symposium on Electronic Commerce and Security 2008 IEEE Conference on 3-5 Aug. 2008.

[4] Sahana K. Bhosale "Architecture of a Single Sign on (SSO) for Internet Banking" Wireless, Mobile and Multimedia Networks, 2008. IET International Conference on 11-12 Jan. 2008.

[5] Dae-Hee Seo, Im-Yeong Lee, Soo-Young Chae and Choon-Soo Kim "Single Sign-On Authentication Model using MAS(Multi-Agent System)" Communications, Computers and signal Processing, 2003. PACRIM. 2003 IEEE Pacific Rim Conference on 28-30 Aug. 2003.

[6] Maryam Eslami Chalandar, Parviz Darvish and Amir Masoud Rahmani "A Centralized Cookie-Based Single Sign-On in Distributed Systems" Information and Communications Technology, 2007. ICICT 2007. ITI 5th International Conference on Dec 2007.

[7] Dan Boneh and Matthew Franklin, "Identity-Based Encryption from the Weil Pairing", SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[8] Louise Owens, Adam Duffy and Tom Dowling, "An Identity Based Encryption System", Proceedings of the 3rd international symposium on Principles and practice of programming in Java, Pages: 154 – 159, Las Vegas, Nevada, 2004.

[9] Vipul Gupta, Sumit Gupta and Sheueling Chang "Performance Analysis of Elliptic Curve Cryptography for SSL" *WiSe'02,* September 28, 2002, Atlanta, Georgia, USA.

[10] Saraiah G, Taqi Ali Syed, Madhu Babu J, Avinash D, Radhesh Mohandas, Alwyn R.Pais "THROTTLING DDOS ATTACKS" SECRYPT 2009, 7 – 10 July. 2009 Milan Italy., in press.