ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Improving Security of Single Sign-On Mechanism for Distributed Service Enviornment

Ragendu .T.B[1], Dr. R. Manimegalai[2]

Student, Department of CSE, Park College of Engineering and Technology, Coimbatore-641659, India[1]

Professor, Department of CSE, Park College of Engineering and Technology, Coimbatore-641659, India [2]

Abstract: Single sign-on (SSO) is a new authentication mechanism that allows users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. The existing scheme is insecure as it fails to meet credential privacy and soundness of authentication. It represents two impersonation attacks. The first attack allows a malicious service provider, who has successfully communicated with a legal user twice, to recover the user's credential and then to impersonate the user to access resources and services offered by other service providers. In another attack, an outsider without any credential may be able to enjoy network services freely by impersonating any legal user or a nonexistent user. In the proposed phase the work is based on to avoid the previous attacks that is impersonation and mounting. Once user enters into the service the portal will assign unique session id for each users with the unique key assignment for every machine. Once user request the service the portal will check the session id and the unique key (RSA signature scheme) for each request.

I. INTRODUCTION

Pervasive computing (ubiquitos/ubicomp) is an advanced computing concept where computing is made to appear everywhere and anywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. A user interacts with the computer, which can exist in many different forms, including laptop computers, tablets, terminals and phones. The underlying technologies to support ubiquitous computing include Internet, advanced middleware, operating system, mobile code, sensors, microprocessors, new I/O and user interfaces, networks, mobile protocols, location and positioning and new materials.

Single sign-on

Single sign-on (SSO) is a mechanism that uses a single action of authentication to permit an authorized user to access all related, but independent software systems or applications without being prompted to log in again at each of them during a particular session. It reduces the risk for the administrators to manage users centrally, increases user productivity by allowing mobility and allows users to access multiple services or applications after being authenticated just once. This doesn't mean that the SSO system unifies account information for all services, applications and systems, rather it hides such a multiplicity of account information into a single account that the user needs to login.

Once the user login, the SSO system generates authentication information accepted by the various applications and systems. In a single sign-on platform, the user performs a single initial (or primary)sign-on to an identity provider trusted by the applications he wants to access.

Benefits of Single Sign-On

1. Reducing password fatigue from different user name and password combinations
2. Reducing time spent re-entering passwords for the same identity
3. Reducing IT costs due to lower number of IT help desk calls about passwords

Types of SSO

The various types of SSO, fall under different categories, based on where they are deployed (Intranet, Extranet, Internet); how they are deployed (architecture – Simple, Complex); the credentials they use (token, certificate..) and the protocols they use (Kerberos, SAML, OpenID.).

Overview of encryption and public-key cryptosystems

Modern cryptosystems are typically classified as either public-key or private-key. Private-key encryption methods, such as the Data Encryption Standard (DES), use the same key to both encrypt and decrypt data.

The key must be known only to the parties who are authorized to encrypt and decrypt a particular message. Public-key cryptosystems, on the other hand, use different keys to encrypt and decrypt data. The public-key is globally available. The private-key is kept confidential.

Digital Signatures

Property of public-key cryptosystems allows a user to digitally "sign" a message they send. This digital signature provides proof that the message originated from the designated sender. In order to be effective, digital signature need to be both message-dependent as well as signer-dependent. This would prevent electronic "cutting and pasting" as well as modification of the original message by the recipient.

Suppose user A wanted to send a "digitally-signed" message, M, to user B:

The RSA algorithm

The Rivest-Shamir-Adelman (RSA) algorithm is one of the most popular and secures public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e, n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a cipher text message C.
3. To decrypt cipher text message C, raise it to another power d modulo n

The encryption key (e, n) is made public. The decryption key (d, n) is kept private by the user.

Cookies and Sessions

A cookie is an information packet generated by a web server and passed to a web browser. It maintains information about the user's habits with regards to the web server by which it has been generated. It does not imply that the user is authenticated.

II. RELATED WORK

Industrial Websites, like many commercial ones, are viewed at different times by disparate users with differing preferences for data organization, display, and access methods[1]. Forcing the data's origin server to accommodate all possible modes and preferences of access unnecessarily burdens the Web server, increases network traffic, increases the number of versions of the database maintained, increases system complexity, and forces multiple servers to implement redundant services. They have proposed the OPES concept regularizes the architecture by encouraging modularity, uniformity, adherence to standards, security, and compartmentalization of knowledg

In this paper, present the Juxtapose (JXTA)-Overlay[2], which is a JXTA-based peer-to-peer (P2P) platform designed with the aim to leverage capabilities of Java, JXTA, and P2P technologies to support distributed and collaborative systems. The platform can be used not only for efficient and reliable distributed computing but also for collaborative activities and ubiquitous computing by integrating in the platform end devices.

The design of a user interface as well as security issues are also tackled. So evaluate the proposed system by experimental study and show its usefulness for massive processing computations and e-learning applications.

By exploiting a smart card[3], this paper presents a robust and efficient password-authenticated key agreement scheme. This paper strengthens the security of the scheme by addressing untraceability property such that any third party over the communication channel cannot tell whether or not he has seen the same (unknown) smart card twice through the authentication sessions.

The proposed remedy also prevents a kind of denial of service attack found in the original scheme. High performance and other good functionalities are preserved.

Our password-authenticated key agreement scheme using smart cards has been really efficient and effective. In terms of efficiency, besides the low communication costs, This solution builds on the efficient cryptographic primitives of secure hash function and symmetric cipher, which may be easily instantiated in and thus inherently viable for smart card environment.

The field bus networks are becoming accessible from the Internet[4], security mechanisms to grant access only to authorized users and to protect data are becoming essential.

This paper proposes a novel, formally-based approach to multilevel analysis of interconnected fieldbus systems, considering both low-level communication protocols and the overall system.. Interactions between the security services offered by the communication protocols and system behavior are formally analyzed, so that it is possible to observe the effects of potential inadequacies of the underlying security protocols on the whole system.

2.1. EXISTING SYSTEM

One user to maintain different pairs of identity and password for different service providers, but this is not practical. Since this could increase the workload of users and service providers as well as the communication overhead of networks. That, after obtaining a credential from a trusted authority for a short period each legal user's authentication agent can use this single credential to complete authentication on behalf of the user and then access multiple service providers.

SSO scheme should meet at least three basic security requirements, enforceability, credential privacy, and soundness. Enforceability demands that, except the trusted authority, even a collusion of users and service providers are not able to forge a valid credential for a new user.

Credential privacy guarantees that colluded dishonest service providers should not be able to fully recover a user's credential and then impersonate the user to log in to other service providers. Soundness means that an unregistered user without a credential should not be able to access the services offered by service providers.

Actually an SSO scheme, has two weaknesses an outsider can forge a valid credential by mounting a credential forging attack since the scheme employed naïve RSA signature without using any hash function to issue a credential for any random identity.

Their scheme is suitable for mobile devices due to its high efficiency in computation and communication.

2.2 Proposed system

In proposed research when the first attack, the "credential recovering attack" compromises the credential privacy in the scheme as a malicious service provider is able to recover the credential of a legal user. The other attack, an "impersonation attack without credentials," demonstrates how an outside attacker may be able to freely make use of resources and services offered by service providers, since the attacker can successfully impersonate a legal user without holding a valid credential and thus violate the requirement of soundness for an SSO scheme.

In proposed signature hiding property of RSA-VES are using to provide the authentication security for SSO. Signature hiding means that an attacker cannot extract a signature from VES without help from the user who encrypted the signature or the trusted authority who can decrypt the VES.

The proposed model achieved significant improvement for valid credential privacy and leaches the violation of soundness. Soundness and signature hiding are the major properties to guarantee a secured digital signature exchange using VES.

2.3 EXPERIMENTAL RESULT

In the next level of approach security issues are going to be considered. The key creations for the specific user identity are differing from the existing system. The Elliptic Curve Digital signature algorithm (ECDS)is used for the effective security. The security issues are discussed about the authentication credentials passing from one service to another. To manage the secure passing of unique credentials this ECDS algorithm is used. This enhanced security application will lead in the secure single sign on in different distributed service environment

III. CONCLUSION

There are two effective impersonation attacks on chang and lee's single sign on scheme. The scheme cannot protect the privacy of a user's credential and a malicious service provider can impersonate a legal user inorder to enjoy the resources and services from other service providers the another attack violates the soundness of authentication by giving an outsider attacker without credential the chance to impersonate even a non-existent user and then freely access resources and service provided by service providers.. The SSO schemes are not give the stronge security guarantee. And this is also vulnerable to these attacks.

Proposed an effective verifiable encryption of RSA signatures, and proposed an improved chang-lee scheme to achieve soundness and credential privacy. As future work, define authentication soundness and construct effective and provably secure single sign-on scheme.

REFERENCES

1. M. W. Condtry and A. C. Weaver , "Distributing Internet Services to the Network's Edge," IEEE Transaction Industrial. Electronics., vol. 50, no. 3, pp. 404–411, June. 2003.

2. L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P Platform for Distributed, Collaborative and Ubiquitous Computing," IEEE Transaction Industrial Electronics., vol. 58, no. 6, pp. 2163–2172, October. 2010.

3. K. Chen, J. Li, X. Li, W. Qiu, and D. Zheng, "Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards," IEEE Transaction Industrial Electronics., vol. 57, no. 2, pp. 793–800, February. 2010.

4. M. Cheminod, A. Pironti, and R. Sisto, "Formal Vulnerability Analysis of a Security System for Remote Fieldbus Access," IEEE Transaction Industrial Information., vol. 7, no. 1, pp. 30–40, February. 2011.

5. M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," IEEE Transaction Industrial Information., vol. PP, no. 99, 2012, DOI 10.1109/TII/2012.2198666.

6. C.-L. Hsu and T.-S.Wu, "Efficient User Identification Scheme With Key Distribution Preserving Anonymity for Distributed Computer Networks," Computer Security, vol. 23, no. 2, pp. 120–125, 2004