Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

Detection of Attacks on Single Sign-On Mechanism for Distributed Computer Networks

Prof. Vaishali Arun Hiray

Dept of Computer Science & Engg, St.mary group Hydearabad,

Abstract — *The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by multiple service providers in a distributed computer network. Recently, Chang and Lee proposed a new SSO scheme and claimed its security by providing well-organized security arguments. In this paper, however, we demonstrative that their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Specifically, we present 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. We identify the flaws in their security arguments to explain why attacks are possible against their SSO scheme. Our attacks also apply to another SSO scheme proposed by Hsu and Chuang, which inspired the design of the Chang–Lee scheme. Moreover, by employing an efficient verifiable encryption of RSA signatures proposed by Ateniese, we propose an improvement for repairing the Chang–Lee scheme. We promote the formal study of the soundness of authentication as one open problem.*

Keywords- *SSO, Databases, Secure Computing, RSA*

I. INTRODUCTION

What is Secure Computing?

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Figure: secure computing

Diagram clearly explain the about the secure computing also Working conditions and basic needs in the secure computing:

If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole.

1. **Physical security:**

Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

Is the place you keep your workplace computer secure enough to prevent theft or access to it while you are away? While the Security Department provides coverage across the Medical center, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when you are not present.

Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of your computer takes account of those risks as well.

2. **Access passwords:**

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled.
To protect your computer, you should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

3. **Prying eye protection:**
   Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.
4. **Anti-virus software:**
   Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, you still need it on the client side (your computer).
5. **Firewalls:**
   Anti-virus products inspect files on your computer and in email. Firewall software and hardware monitor communications between your computer and the outside world. That is essential for any networked computer.
6. **Software updates:**
   It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities.
   Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.
7. **Keep secure backups:**
   Even if you take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.
8. **Report problems:**
   If you believe that your computer or any data on it has been compromised, your should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information.

II. LITERATURE SURVEY

In the context of industrial information technology, the Internet and World Wide Web increasingly are seen as a solution to the problem of providing "anywhere, anytime" services. In the classical view of an Internet-enabled IT infrastructure, services are requested and consumed by a user (e.g., a human requesting plant production data from his or her desktop) and data are provided by an origin server (e.g., a Web server located in a plant that can authenticate users, implement encryption, serve data, and source multimedia streams). This rather simplistic view works well if the number of users is small, the complexity of services required is modest, and the real-time response requirements are lax. However, it fails to scale when one accounts for the complexities of modern networking: many simultaneous users, potentially operating in multiple languages; many complex data types, including incompatible display formats; many differing schemes for implementing privacy and security through many combinations of authentication and encryption. In this paper we propose an alternative-a client/edge server/origin server architecture that can distribute some complex data processing and device interface tasks to a network edge device, the NetEdge. We show how this device can support services thought to be useful to the industrial environment, such as language translation, image transcoding, access device adaptation, virus scanning, content assembly, local content insertion, and caching. The proposal is a win-win situation for all participants: industrial content providers need maintain only one copy of their content, yet consumers are provided with richer services and device-independent interfaces. Although the services provided define the utility of the product, the heart of the Net Edge is its rule engine. Rules specify which service requests, crossing specified processing points, invoke which service callouts. We explore how a proxy let interface connects the rule engine, through Java and C APIs, to the callout engine. We close with performance measurements of the Net Edge throughput and latency characteristics [1].

With the fast growth of the Internet infrastructure and the use of large-scale complex applications in industries, transport, logistics, government, health, and businesses, there is an increasing need to design and deploy multifeatured networking applications. Important features of such applications include the capability to be self-organized, be decentralized, integrate different types of resources (personal computers, laptops, and mobile and sensor devices), and provide global, transparent, and secure access to resources. Moreover, such applications should support not only traditional forms of reliable distributing computing and optimization of resources but also various forms of collaborative activities, such as business, online learning, and social networks in an intelligent and secure environment. In this paper, we present the Juxtapose (JXTA)-Overlay, 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. We evaluate the proposed system by experimental study and show its usefulness for massive processing computations and e-learning applications [2].

User authentication and key agreement is an important security primitive for creating a securely distributed information system. Additionally, user authentication and key agreement is very useful for providing identity privacy to users. In this paper, we propose a robust and efficient user authentication and key agreement scheme using smart cards. The main merits include the following: 1) the computation and communication cost is very low; 2) there is no need for any password or verification table in the server; 3) a user can freely choose and change his own password; 4) it is a nonce-based scheme that does not have a serious time-synchronization problem; 5) servers and users can authenticate each other; 6) the server can revoke a lost card and issue a new card for a user without changing his identity; 7) the privacy of users can be protected; 8) it generates a session key agreed upon by the user and the server; and 9) it can prevent the offline dictionary attack even if the secret information stored in a smart card is compromised [4].

Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards. By exploiting a smart card, this paper presents a robust and efficient password-authenticated key agreement scheme. This paper strengthens the security of the scheme by addressing un traceability 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 [6].

III. *SYSTEM ANALYSIS*

A. Existing System:

The other side, it is usually not practical by asking one user to maintain distinct pairs of identity and password for different service providers, since this could increase the workload of both 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. Intuitively, an 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.

Disadvantages Of Existing System:

- 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.

B. Proposed System

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 real life, these attacks may put both users and service providers at high risk In fact; this is a traditional as well as prudential way to deal with trustworthiness, since we cannot simply assume that beside the trusted authority, all service providers are also trusted. The basic reason is that assuming the existence of a trusted party is the strongest supposition in cryptography but it is usually very costly to develop and maintain. In particular defined collusion impersonation attacks as a way to capture the scenarios in which malicious service providers may recover a user's credential and then impersonate the user to login to other service providers. It is easy to see that the above credential recovery attack is simply a special case of collusion impersonation attack where a single malicious service provider can recover a user's credential. It must be emphasized that impersonation attacks without valid credentials seriously violate the security of SSO schemes as it allows attackers to be successfully authenticated without first obtaining a valid credential from the trusted authority after registration.

Implementation Modules

- User Identification Phase
- Attacks against the Chang–Lee Scheme
- Recovering Attack
- Non-interactive zero-knowledge(NZK)
- Security Analysis

IV. *MODULE DESCRIPTION*

User Identification Phase

To access the resources of service provider, user needs to go through the authentication protocol specified. Here, and are random integers chosen by and, respectively; and are three random nonce; and denotes a symmetric key encryption scheme which is used to protect the confidentiality of user's identity.

Attacks against the Chang–Lee Scheme

The Chang–Lee scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks. The first attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee 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 real life, these attacks may put both users and service providers at high risk.

Recovering Attack

The malicious and then mount the above attack. On the one hand, the Chang–Lee SSO scheme specifies that is the trusted party. So, this implies that service providers are not trusted parties and that they could be malicious. By agreeing with, when they said that "the Wu–Hsu's modified version cold not protect the user's token against a malicious service provider, the work also implicitly agrees that there is the potential for attacks from malicious service providers against SSO schemes. Moreover, if all service providers are assumed to be trusted, to identify him/her user can simply encrypt his/her credential under the RSA public key of service provider. Then, can easily decrypt this cipher text to get 's credential and verify its validity by checking if it is a correct signature issued by . In fact, such a straightforward scheme with strong assumption is much simpler, more efficient and has better security, at least against this type of attack.

Non-interactive zero-knowledge (NZK)

The basic idea of VES is that Alice who has a key pair of signature scheme signs a given message and encrypts the resulting signature under the trusted party's public key, and uses a non-interactive zero-knowledge (NZK) proof to convince Bob that she has signed the message and the trusted party can recover the signature from the cipher text. After validating the proof, Bob can send his signature for the same message to Alice. For the purpose of fair exchange, Alice should send her signature in plaintext back to Bob after accepting Bob's signature.

Security Analysis

The security of the improved SSO scheme by focusing on the security of the user authentication part, especially soundness and credential privacy due to two reasons. On the one hand, the unforgeability of the credential is guaranteed by the unforgeability of RSA signatures, and the security of service provider authentication is ensured by the unforgeability of the secure signature scheme chosen by each service provider.

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user

Will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

ATTACKS AGAINST THE CHANG–LEESCHEME

As can be seen from the previous section, it seems that the SSO scheme achieves secure mutual authentication, since server authentication is done by using traditional RSA signature issued by service provider. *Pj* Without valid credential *Si* it looks impossible for an attacker to impersonate a legal user *Ui* by going through the user authentication procedure

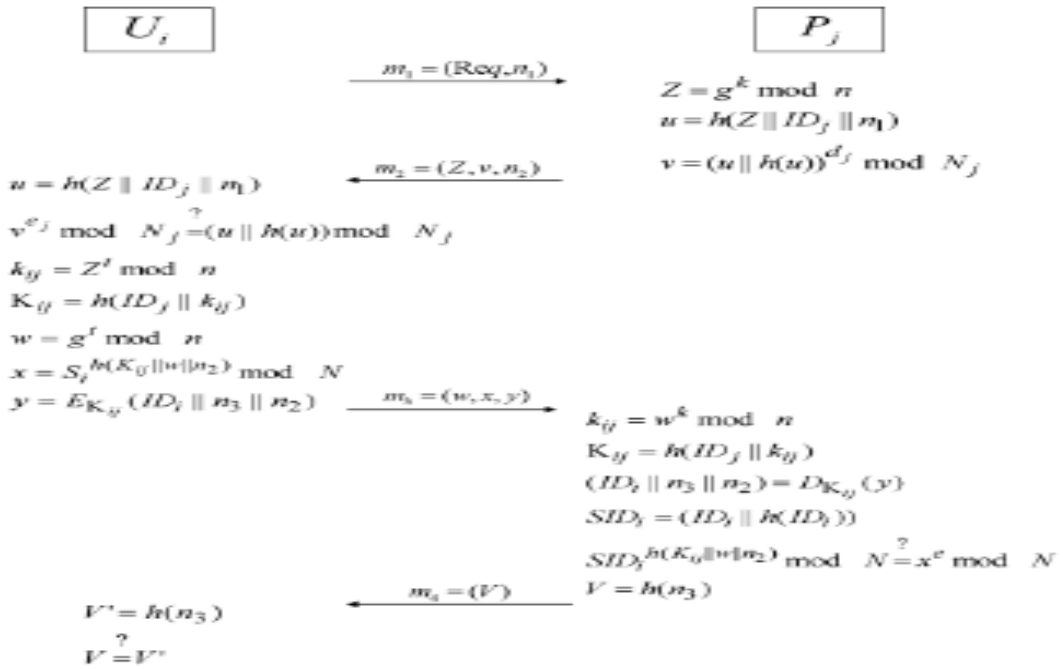

Figure: User identification phase.

It can be seen from the following, however, that the scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks [4].

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 real life, these attacks may put both users and service providers at high risk.

Advantages Of Proposed System:

- The authors claimed to be able to: "prove that and are able to authenticate each other using our protocol." but they provided no argument to show why each party could not be impersonated by an attacker. Second, the authors did discuss informally why their scheme could withstand impersonation attacks.

- The authors did not give details to show how the BAN logic can be used to prove that their scheme guarantees mutual authentication.
- In other words, it means that in an SSO scheme suffering these attacks there are alternatives which enable passing through authentication without credentials.

CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on single sign-on (SSO) scheme. The first attack shows that their scheme cannot protect the privacy of a user's credential, and thus, a malicious service provider can impersonate a legal user in order to enjoy the resources and services from other service providers. The second attack violates the soundness of authentication by giving an outside attacker without credential the chance to impersonate even a non-existent user and then freely access resources and services provided by service providers. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSO scheme proposed in this paper can be formally proven.

REFERENCES

[1]. C. Weaver and M. W. Condtry, "Distributing internet services to the network's edge," *IEEE Trans. Ind. Electron.*, vol. 50, no. 3, pp. 404–411, Jun. 2003.
[2]. L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed, collaborative and ubiquitous computing," *IEEE Trans. Ind. Electron.*, vol. 58, no. 6, pp. 2163–2172, Oct. 2010.
[3]. L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[4]. W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," *Comput. Syst. Sci. Eng.*, vol. 15, no. 4, pp. 113–116, 2000.
[5]. W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 15, no. 6, pp. 2551–2556, Jun. 2008.
[6]. X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.
[7]. M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," *IEEE Trans. Ind. Inf.*, vol. 7, no. 1, pp. 30–40, Feb. 2011.
[8]. A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," *IEEE Trans. Ind. Inf.*, vol. PP, no. 99, 2012, DOI 10.1109/TII/2012.2198666.
[9]. T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Comput. Security*, vol. 23, no. 2, pp. 120–125, 2004.
[10]. Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Comput. Security*, vol. 23, no. 8, pp. 697–704, 2004.
[11]. K. V. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)," *Comput. Security*, vol. 25, no. 6, pp. 420–425, 2006.
[12]. C.-L. Hsu and Y.-H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," *Inf. Sci.*, vol. 179, no. 4, pp. 422–429, 2009.
[13]. B.Wang and M. Ma, "A server independent authentication scheme for RFID systems," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 689–696, Aug. 2012.
[14]. B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacy-enhanced discovery service for RFID-based product information," *IEEE Trans. Ind. Inf.*, vol. 8, no. 3, pp. 707–718, Aug. 2012.

She has completed B.E from S.V.I.T Chincholi nashik Maharashtra. She is Persuing MTECH CSE From ST. Mary Group Institution She is interested in security Area.

