ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Security Analysis of Single Sign on Mechanism for Distributed Computer Network

Ms. K.Lavanya[1], Dr.A.Muthu Kumaravel[*2],

[1] Assistant Professor, Master of Computer Application, Jerusalem College of Engineering, Chennai, India

[2*] Professor& HOD, Master of Computer Application, Bharath University, Chennai, India

ABSTRACT*:* 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 we demonstrate their scheme is actually insecure as it fails to meet credential privacy and soundness of authentication. Here, 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 Attendees, we propose an improvement for repairing the Chang–Lee scheme. We promote the formal study of the soundness of authentication as one open problem.

I.INTRODUCTION

It can be seen from the following, however, that 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. We now first describe our attacks together with the assumptions required, justify why these assumptions are reasonable, and finally discuss why the security analysis are not enough to guarantee the security of the Chang–Lee SSO scheme. From the two attacks presented above, we can learn that both credential privacy and soundness are crucial for SSO.

According to the most traditional form of authentication, a user will be authenticated if he/she can provide a valid pair of user name and password (i.e. credential), and soundness is obviously satisfied because a user is not able to go through authentication without providing a valid credential which is registered and maintained by a server. In complex scenarios, like the Chang–Lee scheme, the situation may be less obvious and, in fact, quite challenging. For this reason, the problem remains an open one for future study. The question of formally defining the soundness of SSO/authentication schemes and rigorously proving them for concrete solutions remains an interesting and important one. Finally, it must be noted that the analysis above shows only that the Chang–Lee SSO scheme fails to achieve secure authentication, without violating its security for achieving user anonymity and session key privacy.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

II. 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 [1]. 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 [2]. 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 [3].

III.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 [4]. 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. [5]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 [6].

IV.MODULE DESCRIPTION

*a. User Authentication Phase***:** To access the resources of service provider, user needs to go through the authentication protocol specified. Here we need to chosen the host or destination to send the data to authorized user .A symmetric key encryption scheme is used to protect the confidentiality of user's identity [7]. In the user identification phase RSA signatures are being checked .To access the resources of service provider, user needs to go through the authentication protocol. Suppose user request for service, service providers generates and return users message which is made by RSA on signature. Once the signature is validated it ensures that user has an authenticated service provider. If user receive any message, service provider checks for confirmation of validity .After that user generates a key temporarily [8-9]. Once you close the process, same key does not work automatically and your session is being stopped.

b. Pair-wise Key Establishment Scheme: A hybrid cryptosystem can be constructed using any two separate cryptosystems: A key encapsulation scheme, which is a public-key cryptosystem, and a data encapsulation scheme, which is a symmetric-key cryptosystem [10]. Pair-wise key establishment involves a sender node can split the to-be-established pair wise secret key into multiple shares and then send them securely over multiple logical paths between itself and recipient nodes. In our simulations, we used a static network. Because a pair wise key establishment usually takes a very short time relative to the velocities between nodes.

*c. Key Distribution scheme Module:*This protocol uses two separate key management schemes; one for group-wide and individual keys and another for sub-network key management. The group-wide key is used for non-critical broadcast messages between Nodes [12]. The individual keys are used for secure communication between nodes creating a sub network and setting up a sub network key. The second key management scheme is creating and distributing the keys for the dynamically created sub networks

*d. 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

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

malicious [14]. 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 [13].

V.FUTURE ENHANCEMENT

We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, we explained why Hsu and Chuang's scheme [12] is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese [11], we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes.

VI.CONCLUSION

In this paper, we demonstrated two effective impersonation attacks on Chang and Lee's 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. We also discussed why their well-organized security arguments are not strong enough to guarantee the security of their SSO scheme. In addition, we explained why Hsu and Chuang's scheme is also vulnerable to these attacks. Furthermore, by employing an efficient verifiable encryption of RSA signatures introduced by Ateniese , we proposed an improved Chang–Lee scheme to achieve soundness and credential privacy. As future work, it is interesting to formally define authentication soundness and construct efficient and provably secure single sign-on schemes. Based on the draft of this work, a preliminary formal model addressing the soundness of SSO has been proposed in. Further research is necessary to investigate the maturity of this model and study how the security of the improved SSOscheme proposed in this paper can be formally proven.

REFERENCES

[1] A. 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] Jayalakshmi T., Krishnamoorthy P., Ramesh Kumar G., Sivamani P., "Optimization of culture conditions for keratinase production in Streptomyces sp. JRS19 for chick feather wastes degradation", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 3(4) (2011) PP.498-503.
[4] L. Lamport, "Password authentication with insecure communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[5] Langeswaran K., Gowthamkumar S., Vijayaprakash S., Revathy R., Balasubramanian M.P., "Influence of limonin on Wnt signalling molecule in HepG2 cell lines", Journal of Natural Science, Biology and Medicine, ISSN : 0976-9668, 4(1) (2013) PP. 126-133.
[6] 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.
[7] 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.
[8] Lydia Caroline M., Vasudevan S.,"Growth and characterization of l-phenylalanine nitric acid, a new organic nonlinear optical material", Materials Letters, ISSN : 0167-577X, 63(1) (2009) pp. 41-44.
[9] 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.
[10] Niranjan U., Subramanyam R.B.V., Khanaa V., "Developing a Web Recommendation System Based on Closed Sequential Patterns", Communications in Computer and Information Science, ISSN : 1865-0929, 101() (2010) PP.171-179.
[11] 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.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

[12] 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.
[13] Anbuselvi S., Jeyanthi Rebecca L., Sathish Kumar M., Senthilvelan T., "GC-MS study of phytochemicals in black gram using two different organic manures", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(2) (2012) PP. 1246-1250.
[14] 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.
[15] B Karthik, TVU Kirankumar, MS Raj, E BharathKumaran,Simulation and Implementation of Speech Compression Algorithm in VLSI, Middle-East Journal of Scientific Research 20 (9), PP 1091-1092, 2013
[16] M.Sundararajan & R.Pugazhanthi," Human finger print recognition based biometric security using wavelet analysis", Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).
[17] .M.Sundararajan & E.Kanniga," Modeling and Characterization of DCO using Pass Transistor", proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)
[18] .M.Sundararajan & C.Lakshmi, "Wavelet based finger print identification for effective biometric security", Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.
[19] .M.Sundararajan, "Optical Instrument for correlative analysis of human ECG and Breathing Signal" Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-I
[20] M.Sundararajan, C.Lakshmi & D.Malathi, "Performance Analysis Restoration filter for satellite Images" Publications of Research Journal of Computer Systems