Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

A Novel Security Analysis against Impersonation Attacks for Distributed Systems

S. B. Hosgoudar[1]*, Aruna A. Daptardar[2], Milind Rao Pawar[3]

[1]Asst. Prof., Department of Computer Science and Engineering, Hirasugar Institute of Technology, Belagavi, India

[2]Asst. Prof., Department of Computer Science and Engineering, Hirasugar Institute of Technology, Belagavi, India

[3]Asst. Prof., Department of Computer Science and Engineering, Hirasugar Institute of Technology, Belagavi, India

Abstract – Distributed systems and networks have been adopted by telecommunications, remote educations, businesses, armies and governments. A widely applied technique for distributed systems and networks is the single sign-on (SSO) which enables an authorized user to use a single secure credential to access multiple services from various service providers. There are many SSO schemes and demonstrated their security by providing well-organized security arguments. However, their scheme is actually insecure as it fails to meet credential privacy and confidentiality of authentication. Specifically, we present two impersonation attacks. The first attack allows a malicious service provider, who has successfully communicated with a authorized user twice, to recover the authorized user's credential and then to impersonate the user to access various services offered by other service providers. In second attack, an attacker without any credential may be able to access the network services freely by impersonating any authorized user. Encryption and decryption of data sent between user and provider can improve security of communication. It also decreases the overhead of the system and would lock out the hackers entering into the system.

Keywords: Authentication, Distributed Computer Networks, Information Security, Security Analysis, Single Sign-on (SSO).

----------♦----------

I. INTRODUCTION

A distributed system is a collection of independent computers that appear to the users of the system as a single computer. Always distributed systems are built up on top of existing networking and operating systems software. To become independent there exist a clear client/server association between two computers in the network. The middleware enables computers to coordinate their activities and to share the resources of the system, so that users perceive the system as a single, integrated computing facility. Thus, middleware is the interface that connects distributed applications across dissimilar physical locations, with dissimilar hardware platforms, network technologies, operating systems, and programming languages. The middleware software is being developed by agreed standards and protocols. It provides standard services such as naming, persistence, concurrency control to ensure that accurate results for concurrent processes are produced and obtained the results as fast as possible. Simple architecture of a distributed system is as shown in below fig 1.1.

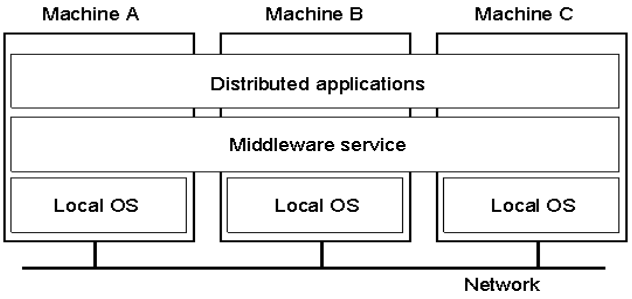


Fig. 1.1 A Distributed System

With the widespread use of distributed computer networks, it has become common to allow authorized users to access various network services offered by various distributed service providers [1]. Consequently, user authentication or user identification plays a crucial role in distributed computer networks to verify if a user is legal and can therefore be granted access to the services requested. To avoid bogus servers, authorized users need to authenticate service providers. After two-way authentication, a session key may be negotiated to keep the confidentiality of the data exchanged

between a user and a service provider. In many cases, the secrecy of legal users must be protected as well. However, practice has shown that it is a big challenge to design efficient and secure authentication protocols with these security properties in complex computer network environments [3].

With the development of distributed computer networks, it is easy for user terminals or computers to share information and computing power with hosts. The distributed locations of service providers make it efficient and convenient for subscribers to access the resources. In general solutions, users must register with each service provider and keep different identity/password pairs for accessing each service provider [14]. However, when users have to keep so much secret information, security problems can occur and increase the overhead for the networks. In a unidirectional identification scheme, an entity identifies the other party by challenging some secret information. In addition, the mutual identification protocol can allow two communicating parties to verify each other. Thus, there are four important security problems that the user identification scheme must solve, i.e., 1) it must determine whether users are legitimate or not; 2) service providers must be authenticated; 3) a common session key must be appropriately established; and 4) the privacy of legal users must be ensured [13]. So the security problems that should be taken into consideration for distributed computer networks include User identification, Key distribution and user anonymity.

User identification is an important access control mechanism for client-server networking architectures. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some of the user identification schemes are proposed for the distributed computer networks. Unfortunately, the most existing schemes cannot preserve user anonymity when possible attacks occur. Also the additional time synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, a secure single sign-on mechanism must be efficient, secure, and suitable for mobile devices in distributed computer networks [13].

Most of the existing schemes are insecure due to impersonation attacks. The common types of attacks are called as credential recovering attack and impersonation attack without credentials. In credential recovering attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers. In impersonation attack without credential, may enable an outside attacker without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services. These two attacks fail to meet credential privacy and soundness, which are essential requirements for SSO schemes and authentication protocols. Security problems that should be taken into consideration for distributed computer networks include: i) User identification (or user authentication): assures one communicating party of the legitimacy of the corresponding party by acquisition of corroborative evidence. ii) Key distribution: a key distribution protocol (or key agreement protocol) is to establish a common secret among two or more communicating parties for subsequent cryptographic use. iii) User anonymity: it conceals the identity of the communicating parties involved in the protocol [12].

II. LITERATURE SURVEY

The classical view of an Internet-enabled IT infrastructure 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 [1]. The security challenges of authenticity, integrity, confidentiality, and execution safety are considered as primary design constraints [2]. As fieldbus networks are becoming accessible from the Internet, security mechanisms to grant access only to authorized users and to protect data are becoming essential. It proposes a formally based approach to the analysis of such systems, both at the security protocols level and at the system architecture level. This multilevel analysis allows the evaluation of the effects of an attack on the overall system, due to security problems that affect the underlying security protocols. A case study on a typical fieldbus security system validates this approach [3].

The anonymity is a desirable security feature in addition to providing user identification and key agreement during a user's login process. Recently, Yang et al., proposed an efficient user identification and key distribution protocol while preserving user anonymity. Their protocol addresses a weakness in the protocol proposed by Wu and Hsu. Unfortunately, Yang's protocol poses a vulnerability that can be exploited to launch a Denial-of-Service (DoS) attack. Here, they crypt analyze Yang's protocol and present the DoS attack. It further secure their protocol by proposing a Secure Identification and Key agreement protocol with user Anonymity (SIKA) that overcomes the above limitation while achieving security features like identification, authentication, key agreement and user anonymity [4] .Performance analyses have shown that efficiency in terms of both computation and communication is not sacrificed in this scheme [5]. User identification is an important access control

mechanism for client-server networking architectures. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some of the user identification schemes are proposed for the distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also the additional time synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, it proposes a secure single sign-on mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks [13].

III. PROPOSED SYSTEM

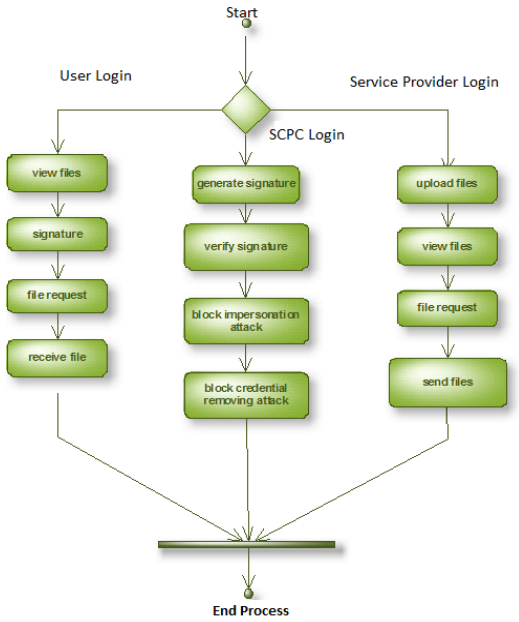
i. Overview of the proposed system

We propose an improvement by employing an RSA-based encryption of signatures, which is an efficient primitive introduced for realizing fair exchange of RSA signatures. Encryption of signatures comprises three parties: a trusted party and two users say Ram and Sham. The basic idea is that Ram 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 noninteractive zero-knowledge (NZK) proof to convince Sham that he has signed the message and the trusted party can recover the signature from the cipher text. After validating the proof, Sham can send his signature for the same message to Ram. For the purpose of fair exchange, Ram should send his signature in plaintext back to Sham after accepting Sham's signature. If he refuses to do so, however, Sham can get his signature from the trusted party by providing Ram's encrypted signature and his own signature, so that the trusted party can recover Ram's signature and sends it to Sham, meanwhile, forwards Sham's signature to Ram. Thus, fair exchange is achieved.

IV. IMPLEMENTATION

Implementation of the project includes single sign-on mechanism, credential recovering attack, impersonation attacks and Smart Card Producing Center. Single sign-on (SSO) is a new authentication mechanism that allows an authorized user with a single credential to be authenticated by multiple service providers in distributed systems. Credential recovering attack is with respect to malicious service provider. In this attack, a malicious service provider who has communicated with an authorized user twice can successfully recover the user's credential. Then, the malicious service provider can impersonate the user to access resources and services provided by other service providers. Impersonation attack is with respect to unauthorized user. This attack may enable an unauthorized user without any valid credential to impersonate a legal user or even a nonexistent user to have free access to the services from various service providers. Smart Card Producing Center is a good example for trusted authority or gateway. In most existing schemes, RSA cryptosystems are used to initialize a trusted authority, called an SCPC (smart card producing center), and service providers. The Diffie–Hellman key exchange technique is employed to establish session keys. The basic idea is each user applies a credential from the trusted authority SCPC, who signs an RSA signature for the user's hashed identity. After that, uses a kind of knowledge proof to show that he/she is in possession of the valid credential without revealing his/her identity to eavesdroppers or to hackers. Actually, this is the core idea of user authentication in most of the SSO schemes.

i. Work Process of the System



Implementation consists of three important phases: Initialization Phase, Registration Phase, and Authentication Phase.

Initialization Phase

SCPC selects two large safe primes p and q to set N = pq. Namely, there are two primes p' and q' such that p= 2p'+1 and q=2q'+1. SCPC now sets its RSA public/private key pair (e, d) such that ed ≡ 1 mod 2p'q', where e is a prime. Let QN be the subgroup of squares in Z*N whose order #G = p'q' is unknown to the public but its bit-length l G = |N| -2 is publicly known. SCPC randomly picks generator g of QN , selects an ElGamal decryption key u , and computes the corresponding public key y = gu mod N . In addition, for completing the Diffie-Hellman key exchange SCPC chooses generator ḡ ϵ Z*N, where n is another large prime number. SCPC also chooses a

cryptographic hash function h (.): {0,1}* □ {0,1}k where security parameter k satisfies 160 ≤ k ≤ |N| - 1. Another security parameter ϵ>1 is chosen to control the tightness of the ZK proof . Finally, SCPC publishes (e,N,h(.),ϵ,g,y, g̃,n), and keeps (d,u) secret.

Registration Phase

In this phase, upon receiving a register request, SCPC gives Ui fixed-length unique identity IDi and issues credential Si = h(IDi)2d mod N. Si calculated as SCPC's RSA signature on h(IDi)2 is an element of QN, which will be the main group we are calculating.

Each service provider Pj with identity IDj should maintain a pair of signing/verifying keys for a secure signature scheme (not necessarily RSA). σj (SKj, Msg) denotes the signature σj on message Msg signed Pj by using signing key SKj . Ver (PK j, Msg, σj) denotes verifying of signature σj with public key PK j, which outputs "1" or "0" to indicating if the signature is valid or invalid, respectively.

Authentication Phase

In this phase, RSA based encryption of signatures is employed to authenticate a user, while a normal signature is used for service provider authentication. The details are illustrated in Fig and further explained as follows.

1) Ui sends a service request with nonce n1 to service provider Pj.

2) Upon receiving (Req, n1), Pj calculates its session key material Z = gk mod n where k ϵ Z*n is a random number, sets u = Z || IDj ||n1, issues a signature v= σj (SKj, u) and then sends m2 = (Z, v, n2) to the user, where n2 is a nonce selected by Pj.

3) Upon receiving m2 = (Z, v, n2), Ui sets u = Z || IDj || n1. Ui terminates the conversation if Ver (PKj, u, v) = 0. Otherwise, Ui accepts service provider Pj because the signature v is valid. In this case, Ui selects a random number t ϵ Z*n to compute w = gt mod n, ki j = h (IDj || ki j). For user authentication, Ui first encrypts his/her credential Si as (P1 = Si . yr mod N, P2 = gr mod N), where r is a random integer with binary length lG. Next, Ui computes two commitments a = (ye) r1 mod N and b = g r1 mod N, where r1 ϵ ± {0,1} is also a random number. After that, Ui computes the evidence showing that credential Si has been encrypted in (P1, P2) under public key y. For this purpose, Ui calculates c = h(Ki j || w || n2 || yer || P2 || ye || g || a || b) and s = r1 – c . r (in Z). Then, x = (P1, P2, a, b, c, s) is the NIZK proof for authentication. Finally, Ui encrypts his/her identity IDi, new nonce n3, and Pj's nonce n2 using session key ki j to get ciphertext CT = Eki j (IDi || n3 || n2), and thereafter sends m3 = (w, x, CT) to service provider Pj.

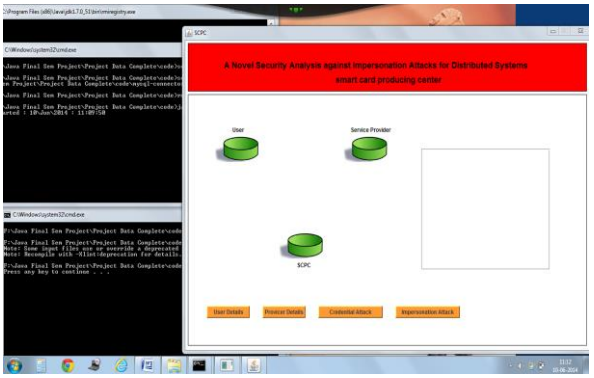
4) To verify Ui, Pj calculates Ki j = wk mod n, the session key Ki j = h (IDj || Ki j), and then uses Ki j to decrypt CT and recover (IDi, n3, n2). Then, Pj computes yer = Pe1 / h(IDi)2 mod N, a = (ye)s . (yer)c mod N, b = gs . Pc2 mod N, and checks if (c, s) ϵ {0, 1}k X ± {0, 1} and c = h(Ki j || w ||n2 || yer || P2 || ye || g || a || b). If the output is negative, Pj aborts the conversation. Otherwise, Pj accepts Ui and believes that they have shared the same session key Ki j by sending Ui m4 = (V) where V = h (n3).

5) After Ui receives V , he checks if V = h(n3). If this is true, then Ui believes that they have shared the same session key Ki j. Otherwise, Ui terminates the conversation.

V. RESULTS AND DISCUSSION

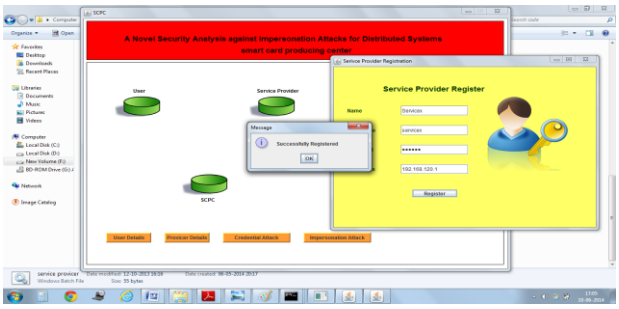
The following steps and snapshots show the actual working scenario and outcomes of this system.

i. SCPC is mainly responsible for the authentication/authorization of user and service provider.

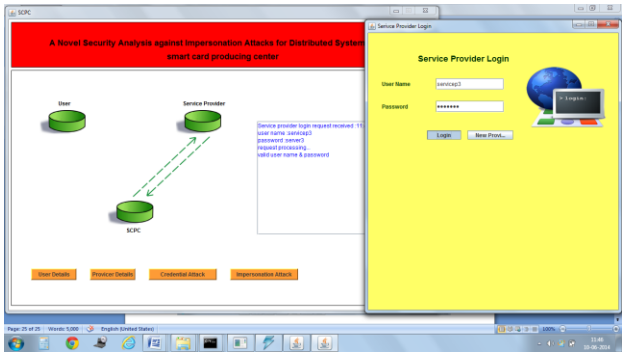


Smart Card Producing Center

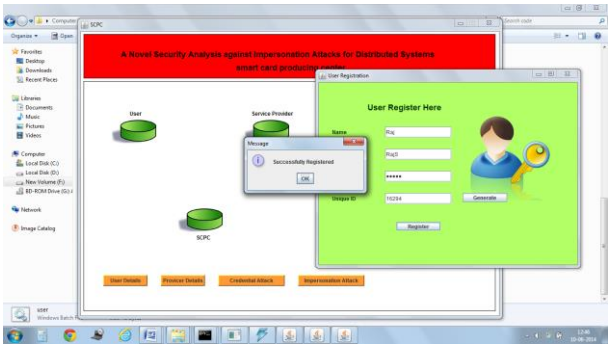
ii. If the service provider is new then registration must be done to get respective credentials to login.



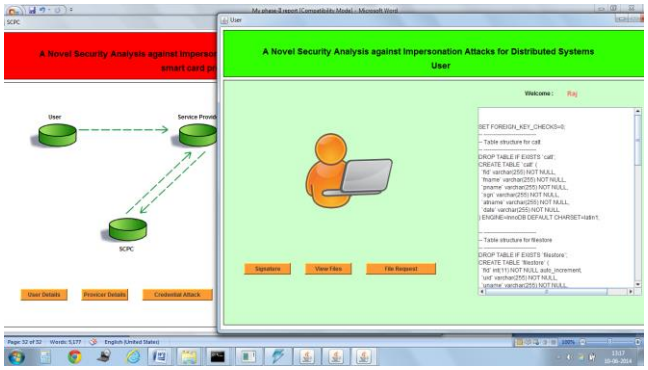
iii. Authentication of service provider by SCPC



iv. If the User is new then registration must be done to get respective credentials to login as shown in below figure.



v. User receives the requested file by entering the necessary details as shown in below



VI. CONCLUSION

Most existing single sign-on schemes in distributed systems suffer from various security issues and are vulnerable to different attacks. We proposed an improvement by employing an RSA based encryption of signatures. It is an efficient primitive introduced for fair exchange of RSA signatures. The proposed single sign on mechanism overcomes the two effective impersonation attacks as credential recovering attack and the impersonation attack without credentials. Our scheme is more secure as it performs the encryption and decryption of data sent between user and service provider to improve the security of communication in distributed systems. It also decreases the overhead of the system and would lock out the hackers entering into the system. It is aimed to provide significant security and privacy in distributed systems.

REFERENCES

A. C. Weaver and M. W. Condtry, “Distributing Internet services to the network’s edge”, IEEE Trans. Ind. Electron., 50(3): 404-411, Jun. 2003.

Y. Xu, R. Song, L. Korba, L.Wang, W. Shen, and S. Y. T. Lang, “Distributed device networks with security constraints,” IEEE Trans. Ind.Inf., vol.1, no. 4, pp. 217–225, Nov. 2005.

M. Cheminod, A. Pironti, and R. Sisto, “Formal vulnerability analysis of a security system for remote field bus access” IEEE Trans. Ind. Informatics, Feb. 2011.

K. V. Mangipudi and R. S. Katti, “A secure identification and key agreement protocol with user anonymity (sika),” Computers and Security, 25(6): 420-425, 2006.

Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, “New efficient user identification and key distribution scheme providing enhanced security,” Computers and Security, 23(8): 697-704, 2004.

B. Fabian, T. Ermakova, and C. Muller, “A privacy-enhanced discovery service for RFID based product information”, IEEE Trans. Ind. Informatics, July 2012.

Anna Squicciarini, Marco Casassa Mont, Abhilasha Bhargav - Spantzel, Elisa Bertino, “Automatic Compliance of Privacy Policies in Federated Digital Identity Management” IEEE Workshop on Policies for Distributed Systems and Networks,2008.

N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE Journal on Selected Areas in Communications, 18(4): 591-606, 2000.

J. Camenisch and M. Michels, “Confirmer signature schemes secure against adaptive adversaries,” in Proc. of EUROCRYPT 2000, LNCS1807, pp. 243-258, Springer, 2000.

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.

Sandeep K. Sood, Anil Sarje and Kuldip Singh “Cryptanalysis of Password Authenticate Schemes: Current Status and Key Issues,” International Conference on Methods and models in Computer Science, 2009.

C. L. Hsu and Y. H. Chuang, “A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks,” Inf. Sci., 179(4): 422-429,2009.

C. C. Chang and C.Y. Lee, “A secure single sign-on mechanism for distributed computer networks,” IEEE Trans. Ind. Electron., 59(1): 629-637, Jan. 2012.

W. C. Ku and S.M. Chen,“Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards,” IEEE Trans. Consum. Electron, vol. 50, no. 1, pp. 204–207, Feb. 2004.

Sabu M. Thampi “Introduction to Distributed Systems” L. B. Institute of Technology for Women, Trivandrum, Kerala, India-695012.

Corresponding Author

S. B. Hosgoudar*

Asst. Prof., Department of Computer Science and Engineering, Hirasugar Institute of Technology, Belagavi, India

E-Mail – shilpahosgoudar.cse@hsit.ac.in