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, Issue 11, November 2014

Single Sign-On Secure Authentication Password Mechanism

Deepali M. Devkate, N.D.Kale

ME Student, Department of CE, PVPIT, Bavdhan, SavitribaiPhule University Pune, Maharashtra ,India.

Assistant Professor, Department of CE, PVPIT, Bavdhan, SavitribaiPhule University Pune, Maharashtra, India.

ABSTRACT: This mechanism allows users to sign on only once and have their identities automatically verified by each application or service they want to access afterwards. Most of application architectures required the user to memorized and utilize a different set of credentials (e.g. username/password or tokens) for each application. The Single sign-on (SSO) is a new authentication mechanism that enables a legal user with a single credential to be authenticated by service providers in distributed computer networks. Impersonation attack and session attack these are the weak points of existing system 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 resources and services offered by service providers may be able to access without authentication by malicious users.In this propose scheme, to preserve credential generation privacy, the trusted authority signs a Schnorr signature on user identity; and to protect credential privacy and soundness, the user exploits his/her id as a signing key to sign a Schnorr signature on the hashed Session key. And by using Advance Encryption Standard key exchange and identification is secure.

KEYWORDS: Credential, SSO, Encryption, Decryption, Schnorr.

I. INTRODUCTION

The aim of this paper is to develop a secure single sign-on mechanism for distributed networks. To make the existing distributed system performs in an efficient, convenient manner and too overcome several possible attacks. In any client/server system, single sign-on is an authentication process that permits multiple applications. But in the existing authentication schemes, it fails to protect the user from several possible attacks when user accessing it..We have proposed a secure single sign-on access control mechanism for Distributed networks to enable the users to login quickly and securely to multiple applications such as websites with just a single identity. In this mechanism, the user can login once for every domain and it also provides only one password which makes it very secured and easy to access the resources from different service providers. It also provides integrity, availability authentication and access control. It could be done by using one way hash function with random nonces.

We have proposed a secure single sign-on access control mechanism for client/server networks to enable the user to login quickly and securely to multiple applications such as websites, mainframe session with just a single identity. In this mechanism the user can login once for every domain and it also provides only one password which makes it very secured and easy to access the resources from different Service providers. It also provides integrity, availability authentication and access control.

II. LITERATURE SURVEY

A.*Anonymity Enhancement on Robust and Efficient Password Authenticated Key Agreement Using Smart Cards*

Our password-authenticated key agreement scheme using smart cards has been really efficient and effective. In terms of effectiveness, it has not only the low communication costs, but also our solution builds on the efficient cryptographic primitives of secure hash function and symmetric cipher, which may be inherently viable for smart card environment. So, this solution not only preserves mutual authentication, key agreement and the functionality of password updating but also can prevent initiator traceability, insider attack, and DoS attack and also blocks them. [3]

B.Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards

We have proposed an efficient and robust user authentication and key agreement scheme that not only can satisfy all the advantages of Fan et al.'s scheme but also can give session key agreement identity protection, low communication and computation cost by using elliptic curve cryptosystems and can prevent the insider attack. Our proposed scheme is very useful in limited computation and communication resource environments to access remote information systems. Also, this scheme can withstand the offline dictionary attack even if the secret information stored in a smart card is eavesdropped [4]

C. Formal Vulnerability Analysis of a Security System for Remote Field bus Access

As field bus networks are becoming accessible from the Internet. So to grant access only to authorized users and to protect data are becoming essential in security point of view. Thus this paper proposes a formally-based approach to the analysis of such systems, not only at the security protocols level, but also at the system architecture level. This multi-level analysis shows the evaluation of the effects of an attack on the whole system, due to security problems that affect the underlying security protocols. This approach can be validated by a case study on a typical field bus security system [5]

D. Review of Security Issues in Industrial Networks

Advanced techniques have been continuously developing for several years to protect office and business networks from information technology-based attacks. But the same has not true for IACS, because of their peculiarities and priorities in security requirements. They make them different from conventional computing systems. So, while superiority in cyber attacks always improves, security management in IACS has remained more or less the same until recently. The interconnection of subsystems throught public communication networks and the Internet, the opening of wireless communication technologies, and the increasing adoption of general-purpose operating systems and s/w available off-the-shelf has then significantly contributed to increase the exposure of IACS to security threats.[6]

E. Distributing Internet Services to the Network's Edge

In the context of industrial information technology, the Internet and World Wide Web are increasingly 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 accessed 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 registered users, implement encryption, serve data, and source multimedia streams).[7]

III. RELATED WORK

A. Node creation phase

In this phase nodes are created and more than 30-50 nodes placed at a particular distance. Wireless nodes placed intermediate area in a distributed network. Each node knows its position relative to the sink. The maximum dimension of node is set as x=4000 and y=4000. The size of the nodes is set as 35 and the ultimate time simulation is 10 ms.The speed of network nodes set as 10-15 m/s.

B. Registration phase

In this phase, node requests the SCPC– smart card producing center for registration. Then SCPC provides a fixed length unique id to all network nodes for identification purpose, this id is generated using RSA signature algorithm which provides a necessary public key and signature to network nodes for its identification process. Every node get a unique id and they are communicated with other nodes using this generated id.

C. Data routing phase

The user and provider establish a communication through multi hop path through the shortest path, the path establishment or path discovery is done through CBR (credit based routing), in the identified path the data is routed from several users through SSO – single sign on mechanism of authenticated user.

D. Authentication phase

In this phase, while a normal signature is used for service provider authentication, RSA-VES is employed to authenticate a user,. Consider an adversary node try to inject false packets to provider in order to confuse the provider about original data packets and also tries to receive the original data packets from user. The RSA – VES algorithm is used to authenticate the original packets, the provider uses private key to decrypt the original data packets.

E. Malicious node detection and legitimate node identification phase

For the proposed malicious node detection process digital signature dynamic source configuration routing is improved, which states KEY SERVER tends to confirm the authentication of provider. By this proposed technique number of users, intermediary nodes and provider can validate each other using dynamic hash function technique. In hash function technique, if user and provider want to verify each other then the USER U generates a hash id through hash function H(n)= PUB_KEY/IDENTITY, i.e. the public key and id of user U generates hash id. In the same way the PROVIDERS generate their hash id. If the user u hash id and provider hash id both are same then the nodes are authenticated for data transmission and authentication.

IV. SYSTEM ARCHITECTURE

Encryption and Decryption between user and provider is ensured using AES algorithm which is more secure than DES and there are currently no known non-brute-force attacks against AES. Data packet send from each provider to user is encrypted and it send to the user, then the user decrypts that packet and the original packet is get back. All these encryption and decryption are done using the more secure Advanced Encryption Algorithm (AES). The implementation is done on the basis of socket programming in Java and which uses server programs and client programs. To execute in different machines, programming is based on IP address of the systems. By using the multithreading features of Java, all the providers can be execute in parallel. The overall checking of authentication of user and provider are explained in fig.1.

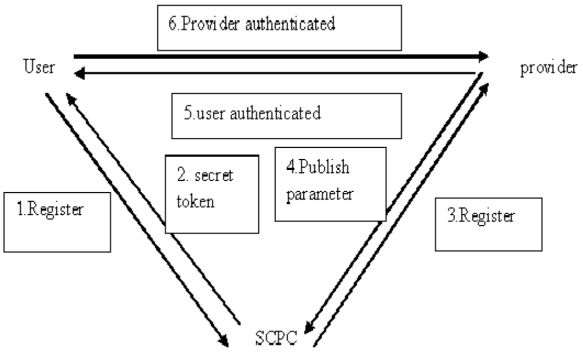

Fig 1. System architecture

V. ALGORITHM

AES is a modern block cipher which supports three key lengths of 128, 192 and 256 bit. It provides excellent long-term security against brute-force attacks. The algorithms scenario is given below. (Fig.2)

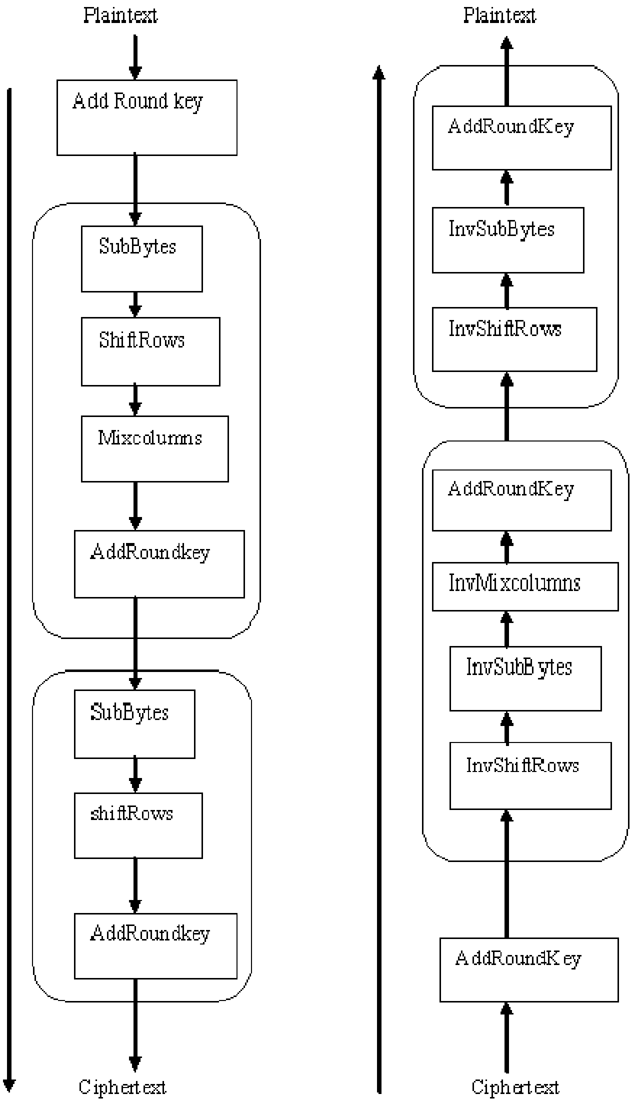

Fig.2. Encryption and decryption in AES

VI. RESULT

A. *Estimated Results*

The results shows that enhanced security for single sign-on solution. It eliminates repeatedly prove identity. Hold different credentials for each application. Here, two attacks are detected i.e. impersonation attack and session attack. So here malicious users are detected and also blocked.

VII. CONCLUSION

This paper proposes a single-sign-on mechanism based on AES algorithm which more secure than DES algorithm used in chang-Lee scheme.AES is the most widely used symmetric cipher today.It provides excellent long-term security against brute-force attacks. Thus when security is taken into consideration AES is given priority than other algorithms. AES is resistant to all known attacks. Encryption and decryption of data sent between used and provider can improve security of communication. For encryption and decryption same key is used at both sides.AES is certified by US govt. By using this scheme in single-sign-on mechanism user need single credential for access to all applications and services provided by system. It would detect the malicious users entering into the system and lock them.

REERENCES

[1] C. Ramkrishnan, S. Dhanabal, "Security analysis of a single sign-on mechanism for distributed computer networks"IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, pp146-149,June 2014

[2] Jean Jacob, Mary John , "Security enhancement of a single sign-on mechanism for distributed computer networks",IJMER, vol. 3, pp-1811-1814, June 2013

[3] 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.

[4] 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.

[5] M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote field bus access," IEEE Trans. Ind. Inf., vol. 7, no. 1, pp. 30–40, Feb. 2011.

[6] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol. PP, no. 99, 2012] 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.

[7]] 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.

[8] W. Stallings, "Cryptography and Network Security", 4th ed. Upper Saddle River, NJ: Pearson, pp. 334–340,Nov. 2005.

[9] Advanced Encryption Standard, NIST Std. FIPS PUB 197, 2001