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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

A Productive Arrangement for Smart Card Based on Password-Authentication Using Key Agreement

S. Gayathri[1], D. Pavithra[2], T. Sivaranjani[3],

Assistant Professor, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Chennai, Tamil Nadu, India

B.E, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Chennai, Tamil Nadu, India

B.E, Department of Computer Science and Engineering, Jeppiaar SRR Engineering College, Padur, Chennai, Tamil Nadu, India

ABSTRACT: Remote authentication is of great importance to protect a networked server against malicious remote users in distributed systems. The proposed system initiates the study of two specific security threats on smart-card-based password authentication in distributed systems. A smart-card-based password authentication scheme involves a service provider and a service requester, and typically consists of three phases. Smart-card-based password authentication is widely used in security mechanisms to determine the remote client, who must hold a valid smart card and password to carry out authentication with the server. Using two recently proposed protocols as case studies, we demonstrate two new types of adversaries with smart card adversaries with pre-computed data stored in the smart card adversaries with different data (with respect to different time slots) stored in the smart card. These threats, though realistic in distributed systems, have never been studied in the literature. In addition to point out the vulnerabilities, we propose the countermeasures to thwart the security threats and secure the protocols.

KEYWORDS: Key Exchange, Authentication-Procedures, Offline Dictionary Attack, Online Dictionary Attack, SmartCard.

I. INTRODUCTION

The main objective of this proposed work is to avoid Use of Active Attack And Passive Attack (Online and Offline attack based)for this purpose we presents a single card number which allows to access the bank accounts. As well as the major scope of this system is to give security for transaction purpose and provide single card number to remember instead of remembering stored in smart card itself. In this modern era, organizations greatly rely on computer networks to share information throughout the organization in an efficient and productive manner. Organizational computer networks are now becoming large and ubiquitous. Assuming that each staff member has a dedicated workstation, a large scale company would have few thousands workstations and many server on the network. Network security is a big topic and is growing into a high profit le (and often highly paid) Information Technology (IT) specialty area. Security-related websites are tremendously popular with savvy Internet users.

The popularity of security-related certifications has expanded. Esoteric security measures like biometric identification and authentication – formerly the province of science fi ction writers and perhaps a few ultra-secretive government agencies – have become commonplace in corporate America. Yet, with all this focus on security, many

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

organizations still implement security measures in an almost haphazard way, with no well-thought-out plan for making all the parts fi t together. Computer security involves many aspects, from protection of the physical equipment to protection of the electronic bits and bytes that make up the information that resides on the network. It is likely that these workstations may not be centrally managed, nor would they have perimeter protection.

They may have a variety of operating systems, hardware, software, and protocols, with different level of cyber awareness among users. Now imagine, these thousands of workstations on company network are directly connected to the Internet. This sort of unsecured network becomes a target for an attack which holds valuable information and displays vulnerabilities. A network is defined as two or more computing devices connected together for sharing resources efficiently. Further, connecting two or more networks together is known as internetworking. Thus, the Internet is just an internetwork – a collection of interconnected networks.

For setting up its internal network, an organization has various options. It can use a wired network or a wireless network to connect all workstations. Nowadays, organizations are mostly using a combination of both wired and wireless networks. In a wired network, devices are connected to each other using cables. Typically, wired networks are based on Ethernet protocol where devices are connected using the Unshielded Twisted Pair (UTP) cables to the different switches. These switches are further connected to the network router for accessing the Internet. In wireless network, the device is connected to an access point through radio transmissions. The access points are further connected through cables to switch/router for external network access.

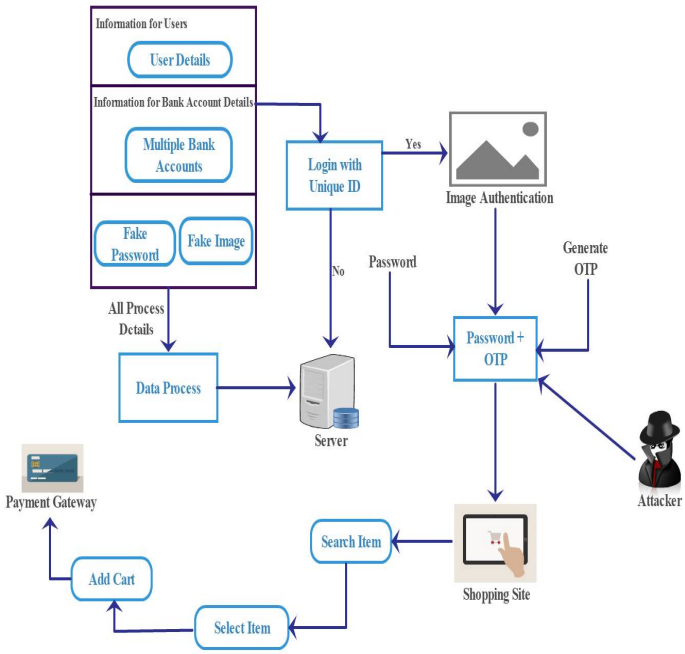

Fig.1 Block Diagram of the Proposed System

Wireless networks have gained popularity due to the mobility offered by them. Mobile devices need not be tied to a cable and can roam freely within the wireless network range. This ensures efficient information sharing and boosts productivity. The common vulnerability that exists in both wired and wireless networks is an "unauthorized access" to a network. An attacker can connect his device to a network though unsecure hub/switch port. In this regard, wireless network are considered less secure than wired network, because wireless network can be easily accessed without any physical connection. After accessing, an attacker can exploit this vulnerability to launch attacks such as: •

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

Sniffing the packet data to steal valuable information. •Denial of service to legitimate users on a network by flooding the network medium with spurious packets.• Spoofing physical identities (MAC) of legitimate hosts and then stealing data or further launching a 'man-in-the-middle' attack.

II. PROBLEM SUMMARY AND RESOLUTION

In the existing approaches, many smart-card- based password authentication schemes have been proposed and various security goals and properties have been addressed, including (but are not limited to) low computation and communication cost, no password table, security against replay attacks, security against parallel session attacks, mutual authentication, session key agreement and security against adversaries with smart card. It is not trivial to design smart-card- based password authentication satisfying even the basic security requirements, and in fact many schemes have been found broken shortly after their proposals.

The existing approach has several demerits, which are summarized as below:

(i) A user is allowed to choose his/her password in the password-changing phase.

(ii) It is well a known problem that human memorable passwords only come from a small domain. Which a known as dictionary attack. Dictionary attack can be further divided into online (active) and offline (passive) dictionary attack.

In the proposed approach, two smart-card- based password authentication schemes were proposed. Juang, Chen andLiaw described a robust and efficient user authentication and key agreement scheme using smart cards. Juang-Chen- Liaw's scheme can be viewed as an improvement over the one proposed, which is designed to accommodate a number of desirable features including no password table, server authentication, etc. But the major limitation of is a relatively high computation cost.

This is improved with a new proposal in by exploiting the advantages of pre- computation, Juang-Chen-Liaw's scheme was further improved by Sun etal.who shows that attackers can successfully impersonate the user with old password and old data in the smart card. Thus, a new scheme was proposed to fix that flaw, together with several other new properties such as forward secrecy and password changing without any interaction with the server. The security analysis made indicates that the improved scheme remains secure under offline- dictionary attack in the smart-card- loss case.

The proposed system contains several merits, which are summarized as below:

(i) Costly operations are completed in the offline-phase (before the authentication).

(ii) It is claimed in that their scheme can prevent offline dictionary.

(iii) Attacks even if the secret information stored in a smart card is compromised.

III. SYSTEM IMPLEMENTATIONS

The system is implemented by means of the following modules that are described clearly by means of the following summary.

A. Anti-Access Module

An attacker on a smart-card-based password authentication protocol should not be able to make log-in either only with the smart card or with the password). As well as to capture these requirements we define the potential attacker from two aspects namely the behavior of the attacker and the information compromised by the attacker. A smart-card-based password authentication protocol may be faced with a passive attacker (the attacker can observe messages by eavesdropping) and an active attacker (active attacker inject and modify messages). An active attacker can also request any session keys adaptively so it is evident that an active attacker is more powerful than a passive attacker.

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 1, January 2018

B. Session-Key Determination

A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications. A Session keys are sometimes called symmetric keys, because the same key is used for both encryption and decryption. A session key may be derived from a hash value using the CryptDeriveKey function (this method is called a session-key derivation scheme). Throughout each session, the key is transmitted along with each message and is encrypted with the recipient's public-key. Session keys are changed frequently and different session key may be used for each message.

C. Flaws Detection

A successful attack against the session key will undermine the security of whole system from at least two aspects. First the communication between the user and the server is no longer secure if Sk is compromised. Second the adversary can freely change the user's password. The attack is different from the common offline dictionary attack with the smart card. Since the adversary is able to change the password with the session key Sk once the log-in phase is completed , the adversary can immediately change the password and can successfully login to the server.

D. Password Determination

A passive attacker can also successfully find the user's current password using offline dictionary attack. In the log-in phase, the smart card sends the server a message This message can assist an offline-dictionary attacker to verify if the guess of the password (i.e.PWi) is correct.

E. Password Changing Phase

The new scheme provides the usability of password-changing operations and has several desirable key properties. The password can be changed without any interface with the server the user enters the old password with the new password to change the password.

In this system, we studied the problem of tracking and predicting user's adoption rates of products in a competitive market. We first introduced a flexible factor-based decision function to capture the change of user's product adoption rate over time, where various factors from heterogeneous data sources can be generally leveraged. Using this factor based decision function, we developed the models by assuming the generalized and personalized user preference respectively. Furthermore, we presented how to leverage product competition effect into the models, and designed the models by simultaneously learning product competition and user's preferences with both generalized and personalized assumptions. Finally, the experimental results on two real-world datasets clearly validated the effectiveness and efficiency of our proposed models.

IV. LITERATURE SURVEY

In the year of 2011, the authors "X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R.H. Deng" proposed a paper titled "'A Generic Framework for Three-Factor Authentication: Preserving Security And Privacy in Distributed Systems", in that they described such as: as a component of the security inside dispersed frameworks, different administrations and assets require insurance from unapproved utilize. Remote verification is the most generally utilized strategy to decide the character of a remote customer. This paper explores an orderly approach for validating customers by three variables, specifically secret word, brilliant card, and biometrics. A non specific and secure system is proposed to update two-factor confirmation to three-factor verification. The change not just essentially enhances the data confirmation with ease yet in addition ensures customer security in circulated frameworks. What's more, our system holds a few practice-accommodating properties of the basic two-factor validation, which we accept is of autonomous intrigue.

In the year of 2012, the authors "R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen" proposed a paper titled "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", in that they described such as: infusing false information assault is a notable genuine risk to remote

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

sensor organize, for which a foe reports fake data to sink causing mistake choice at upper level and vitality squander in on the way hubs. In this paper, we propose a novel transfer speed effective helpful verification (BECAN) plot for sifting infused false information. In light of the arbitrary chart attributes of sensor hub organization and the helpful piece packed validation system, the proposed BECAN plan can spare vitality by early recognizing and sifting the greater part of infused false information with minor additional overheads at the on the way hubs. Likewise, just a little part of infused false information should be checked by the sink, which in this manner generally lessens the weight of the sink. Both hypothetical and reproduction comes about are given to show the viability of the proposed conspire regarding high sifting likelihood and vitality sparing.

In the year of 2011, the authors "K. Xi, J. Hu, and F. Han" proposed a paper titled "Mobile Device Access Control: An Improved Correction Based Face Authentication Scheme and Its Java ME Application", in that they described such as: the least difficult strategy for recognizing a server is to depend on the Domain Name System (DNS) or even TCP/IP tending to. As a designer, you accept that when your customer application endeavors to interface with a named server, as somehost.com, your customer application is associated with the right server. This is a truly enormous suspicion. The way from your customer application to the server is probably going to incorporate PCs and hardware about which you know alongside nothing. For security purposes, you can expect that at least one of these machines is worked by culprits who can see all activity going between your customer and the server. A maverick machine could be utilized for a man-in-the-center assault, enabling assailants to view and record all activity amongst you and the server. Utilizing a similar machine, assailants could even change movement amongst you and the server or simply imitate the server out and out. There are known methods for mocking DNS queries and even IP addresses. Without cryptographic validation strategies, customers can't recognize a phony server from the genuine one.

V. CONCLUSION

This system returned to the security of two secret key verified scratch understanding conventions utilizing brilliant cards. While they were thought to be secure, we demonstrated that these conventions are imperfect under their own suppositions individually. Specifically, we considered a few kinds of enemies which were not considered in their outlines, e.g., adversaries with precomputes information put away in the brilliant card and foes with distinctive information (as for various schedule vacancies) put away in the SmartCard. These enemies speak to the potential dangers in conveyed frameworks and are not the same as the usually known ones, which we accept merit the consideration from both the scholarly world and the industry. We also proposed the arrangements to settle the security defects. By and by, our outcomes feature the significance of expounds security models and formal security examination on the outline of secret word confirmed key assertion conventions utilizing Smartcards.

REFERENCES

[1] K.-K.R. Choo, C. Boyd, and Y. Hitchcock, ‘‘The Importance of Proofs of Security for Key Establishment Protocols: Formal Analysis of Jan-Chen, Yang-Shen-Shieh, Kim-Huh-Hwang-Lee, Lin-Sun-Hwang, Yeh-Sun Protocols,’’ Comput. Commun., vol. 29, no. 15, pp. 2788-2797, Sept. 2006.
[2] H. Chien, J. Jan, and Y. Tseng, ‘‘An Efficient and Practical Solution to Remote Authentication: Smart Card,’’ Comput. Security, vol. 21, no. 4, pp. 372-375, Aug. 2002.
[3] T.F. Cheng, J.S. Lee, and C.C. Chang, ‘‘Security Enhancement of an IC-Card-Based Remote Login Mechanism,’’ Comput. Netw., vol. 51, no. 9, pp. 2280-2287, June 2007.
[4] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, ‘‘Robust Remote Authentication Scheme with Smart Cards,’’ Comput. Security, vol. 24, no. 8, pp. 619-628, Nov. 2005.
[5] J.Hu, D. Gingrich, and A. Sentosa, ‘‘A k-NearestNeighbor Approach for User Authentication Through Biometric Keystroke Dynamics,’’ in Proc. IEEE ICC Conf., Beijing, China, May 2008, pp. 1556-1560.
[6] C.L. Hsu, ‘‘Security of Chien et al.’s Remote User Authentication Scheme Using Smart Cards,’’ Comput. Stand. Interfaces, vol. 26, no. 3, pp. 167-169, May 2004.
[7] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R.H. Deng, ‘‘A Generic Framework for Three-Factor Authentication: Preserving Security And Privacy in Distributed Systems,’’ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390-1397, Aug. 2011.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 1, January 2018

[8] W.S. Juang, S.T. Chen, and H.T. Liaw, ''Robust and Efficient Password Authenticated Key Agreement Using Smart Cards,'' IEEE Trans. Ind. Electron., vol. 55, no. 6, pp. 2551-2556, June 2008.
[9] 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.
[10] P.C. Kocher, J. Jaffe, and B. Jun, ''Differential Power Analysis,'' in Proc. Adv. CRYPTO, vol. LNCS 1666, M.J. Wiener, Ed., 1999, vol. LNCS 1666, pp. 388-397.
[11] L. Lamport, ''Password Authentication with Insecure Communication,'' Commun. ACM., vol. 24, no. 11, pp. 770-772, Nov. 1981.
[12] C. Lee, M. Hwang, and I. Liao, ''Security Enhancement on a New Authentication SchemewithAnonymity forWireless Environments,'' IEEE Trans. Ind. Electron., vol. 53, no. 5, pp. 1683-1687, Oct. 2006.
[13] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, ''BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 1, pp. 32-43, Jan. 2012.
[14] S.W. Lee, H.S. Kim, and K.Y. Yoo, ''Improvement of Chien et al.'s Remote User Authentication Scheme Using Smart Cards,'' Comput. Stand. Interfaces, vol. 27, no. 2, pp. 181-183, Jan. 2005.
[15] J.Y. Liu, A.M. Zhou, and M.X. Gao, ''A New Mutual Authentication Scheme Based onNonce and Smart Cards,'' Comput.Commun., vol. 31, no. 10, pp. 2205-2209, June 2008.
[16] J. Liu, Z. Zhang, X. Chen, and K.S. Kwak. (2014, Feb.). Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks. IEEE Trans. Parallel Distrib. Syst. [Online]. 25(2), pp. 332-342. Available: http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.145.
[17] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, ''Examining Smart-Card Security Under the Threat of Power Analysis Attacks,'' IEEE Trans. Comput., vol. 51, no. 5, pp. 541-552, May 2002.
[18] H.S.Rhee, J.O. Kwon, andD.H. Lee, ''ARemoteUserAuthentication Scheme withoutUsing SmartCards,'' Comput. Stand. Interfaces, vol. 31, no. 1, pp. 6-13, Jan. 2009.
[19] H. Sun, ''An Efficient Remote User Authentication Scheme Using Smart Cards,'' IEEE Trans. Consum. Electron., vol. 46, no. 4, pp. 958-961, Nov. 2000.
[20] D.Z. Sun, J.P. Huai, J.Z. Sun, J.X. Li, J.W. Zhang, and Z.Y. Feng, ''Improvements of Juang et al.'s Password-Authenticated Key Agreement Scheme Using Smart Cards,'' IEEE Trans. Ind. Electron., vol. 56, no. 6, pp. 2284-2291, June 2009.