A Survey OnAuthenticated Key And File Exchange Protocol For Secure Network Communication

ReshmiVijayan
PG Student ,Information&Technology
Govt .EnggCollegeBarton Hill ,
Trivandrum ,India.
reshmivijayan30594@gmail

SreedivyaR S
Assistant Professor,
Information & Technology
Govt .EnggCollegeBarton Hill
Trivandrum ,India.
rssreedivya@gmail.com

ABSTRACT

AuthenticatedKey Exchange (AKE) protocolallowsauser anda server toauthenticateeachother andgeneratea sessionkey forthesubsequent communications.However, mostof them have one or more weaknesses,suchas vulnerability againstlost-smart-card attack,offlinedictionary attack,de-synchronizationattack,or lackof forward secrecy,useranonymity oruntraceability. Furthermore,anAKE scheme under the publickey infrastructuremay notbe suitablefor lightweightcomputational devices,andthesecurity modelofAKE does not captureuseranonymityandresist lost-smart-card attack.Understanding securityfailures ofcryptographic protocolsisthekey tobothpatching existingprotocolsanddesigning future schemes.Then,we analyze anefficient dynamicID-basedscheme withoutpublic-key operations.Thisproposalattemptsto overcome many of the well-known security andefficiencyshortcomingsof previous schemesandsupports more functionalities than its counterparts. In thispaper,weproposeanoveldynamic ID-based AnonymousTwo-Factor AKE protocol whichaddresses all theabove issues.The lowcomputationaland bandwidthcostindicatesthatour protocol canbe deployed for pervasivecomputing applicationsandmobilecommunications in practice.

1. INTRODUCTION

With the rapid development of low-powerandhighly efficientnetworks, mobileuserscanpay bills,buy goods online, and carry out electronic transactions by subscribingtovarious remote services. Though mobilecomputingdevicesarehighly portable, theyareusuallyunprotectedandeasyto bestolenorgetlost.Unlessprecautions are taken, an unauthorized person may gainaccesstothe informationstored on them.Forinstance,illegalaccessmay be acquired by intruders if the data is "sniffedoutoftheair" inwireless communicationsor some malware is installed.The lackof authenticationand privacy may causeevenmoresevere resultslike crippleddevices,personaldata loss,disclosure of non-public data,or chargeof abusedusageagainstthedevice owner.Mobilecomputing devicesareof greatsecurityconcernnotonly becauseof thedatastoredonthem,butalsofor that they may provideaccesstootherservices thatstoreordisplay non-publicdata.For almostallthese transactions,mutual authenticationanduserprivacy are required in the key exchange before remoteserversstartproviding servicesto users.In particular, authentication and privacy play animportantrolein applicationsfor industrialnetworks, wirelesssensor networks,distributed networks,aswellasRFIDsystems.Due totheadvantagesonportability and usability, most proposed authenticated key exchange (AKE) protocols support twofactorauthenticationusing passwords andsmartcards,especially withthe evolution of contactless smart card towards the NFC(near-field communication)technology recently. Thereare twomainattacksthatasecure two-factorAKE protocolhastodefend against:Lost-Smart-Card Attackand OfflinePassword DictionaryAttack.

Informally,userprivacy refersto theanonymityanduntraceability ofa user's identityas well as the corresponding smartcardintheprotocol executions.Anonymity aimstoprotectthe locationand activities of the user, while untraceabilitypreventsanadversaryfrom linking twosessionstothesameuser. Thoughtraceability maynotallowan adversary toidentify a user directly, it may helptheadversarytoprofileauser, forexample,revealtheemailserverand the bankaccountoftheuser, ortheonline shopping mallthattheuserusedtovisit. Hencethe main researchproblemontwo-factorAKE nowadaysistoconstructa schemethatsupportsuseranonymity and untraceabilityandpreservessecurity againstbothlost-smart-card attackand offlinedictionaryattack.AdynamicID-based remote userauthenticationscheme usingsmartcardstoremedy the weaknesses in thepassword-based authenticationschemes.The scheme allowedusers tochoose andchange their passwordsfreely anddidnotneedto maintainany verifiertable.They claimed thattheir scheme wassecure againstID-theft,andcouldresistforgery attacks, replay attacks,insiderattacks,guessing attacks and stolen verifier attacks.

2.LITERATURE REVIEW

In2005, Fan etal.[1]proposed a two-factor authentication protocol that fails to achieve user anonymity and sessionkeyestablishment.Asitisbased onRabin'spublickeycryptosystem,Fan etal.'sscheme islessefficientwhen compared withrecentresults based on elliptic curvecryptosystems.

In2004Dasetal.[2] proposeda dynamic ID-based password authentication scheme.Password-based authentication schemes are the most widely usedtechniquesforremote userauthentication.Many staticID-based remote userauthenticationschemesboth withandwithoutsmartcards have been proposed. Mostoftheschemesdo not allow the users tochooseandchangetheir passwords,andmaintaina verifier table to verifythevalidity oftheuserlogin.Inthis paper present a dynamicID-basedremote userauthenticationschemeusing smart cards. The schemeallowsthe users to chooseandchange theirpasswordsfreely, and donot maintain any verifier table. The schemeissecureagainstID-theft,and can resist the reply attacks, forgery attacks,guessingattacks,insider attacks and stolen verifier attacks.

In2013Wang etal.[3] showedthatmany recently proposeddynamicID-based AnonymousTwo-factorAKE protocols have one or more weaknesses,suchas vulnerability against lost-smart-card attack,offlinedictionary attack,orlack of forwardsecrecy,anonymity and untraceability .Itisworthnotingthat,in ordertoprovideuseranonymity,almost all dynamicID-based two-factor authentication protocolsneed an additional synchronization mechanismto maintaintheconsistency oftheone-time identity betweentheuserandtheserver. However, this consistency is broken easily,andtheusermay nolongerbeable to login theserver.

In2015,2016Chaudhryetal.proposed twoschemes[4],[5]thatareclaimedto achieve anonymity and many other desirable properties, but both of them don’tsupportsmartcardrevocation,and thesecondscheme[5]doesnotprovide passwordchangemechanism.Besides,we foundthatthefirstscheme[4]failedto achieve forward secrecy even though it claimedso,becauseitsprevioussession keys can be recovered if the adversary getsaccesstotheuser’spassword,smart card and protocol transcripts of previous sessions. There are also some other schemesbasedonbiometrictechniquesor adjustedforthesettingofmultipleservers [6],[7],whichisofindependentinterest but out of the scope of this paper. Furthermore, theschemes under public keyinfrastructuremaynotbesuitablefor lightweight computation devices. Therefore, itis stillan open problem to designasecureandefficientAnonymous Two-Factor AKEscheme without using publickeys.

3.FUNCTIONALITY AND PERFORMANCE COMPARISONS

3.1 FunctionalityComparison

Incomparisonoffunctionalities,we focus onthesecurity against offlinedictionary attack,anonymity anduntraceability, mutualauthenticationandkey exchange, forward secrecy,supportof password change,anddependenceonthe public key infrastructure.

3.2 Performance Comparison

IntheLoginandAuthenticationphase of ourscheme,itrequiresthree ellipticcurve scalar multiplicationstocompute(e;c), where ecan be pre-computed; and six hash operations..Itrequires threeelliptic curve scalarmultiplications to compute (d;c),where dcanbeprecomputed;two block encryptions and five hash operationsfor getting andverifying inthe server.

	Anonymity enhancement on Robust and efficient password-authenticatedkey agreement scheme using smart cards	Preserving privacy for free Efficientand provably secure two-factor authenticationscheme with user anonymity.	Provably Secure Dynamic ID-based Anonymous Two-factor AuthenticatedKey Exchange Protocol with Extended Security Model
No password table	**Y**	**Y**	**Y**
No server’s publickey	**N**	**N**	**Y**

Mutual authentication and Key agreement	**Y**	**Y**	**Y**
Forward secrecy	**N**	**N**	**Y**
Anonymity or untraceability	**Y**	**Y**	**Y**
Password change	**Y**	**N**	**Y**

CONCLUSION

The proposedananonymoustwo-factor AKE schemewhich preserves security againstvariousattacksincluding de-synchronization attack andpasswordguessing attack,and supportsseveraldesirable properties including perfectforward secrecy, anonymity oruntraceability,adaptively passwordchange,nocentralized password storage,andnolong-term publickey. Furthermore, ourprotocol maintain high efficiencyintermsofstoragerequirement, communication cost as wellas computationalcomplexity.The protocol requiresonly afewnumberofmessage flowsandallthe transmittedmessagesare short insize.Additional,the proposed schemeisprovablysecureinourextended security modelofAKE.Therefore,the proposedscheme issuitable for deploymentin various low-power networks,inparticular, the pervasiveand mobile computing networks. The enhanced scheme also ensures privacyand anonymity.Althoughthe scheme incurs someextra memory,communication,and computationcostbecause of storage and communicationof user’spseudo-identity, yetitisonly becauseofthisadditional burden thatthe proposedscheme isableto resistuseranonymity violationattackand smart cardstolenattack.

REFERENCES

[1] C. Fan, Y. Chan, andZ. Zhang, "Robust remote authentication schemewithsmartcards," Comput.Secur.,vol.24,no.8,pp.619-628, Nov. 2005..

[2] M. L. Das, A. Saxena, andV. P. Gulati, "A dynamicID-based remote user authenticationscheme,"IEEE Trans.Consum. Electron., Vol. 50, no. 2, pp.629-631, 2004.

[3]S.Chaudhry,M.S.Farash,H.Naqvi, S.Kumari,andM.K. Khan,"An enhanced privacypreserving remote user authenticationscheme with provablesecurity",Security Comm. Networks, 8:3782-3795,2015.

[4] S.Chaudhry,H. Naqvi,K. Mahmood, H. F. Ahmad, and M. K. Khan, "An ImprovedRemote User Authentication Scheme Using EllipticCurve Cryptography", Wireless Pers. Commun.,DOI 10.1007/s11277-016-3745-3, 2016.

[5] S. Chaudhry, "A secure biometric based multi-serverauthentication scheme for socialmultimedia networks", MultimedTools Appl., 75:12705-12725, 2016.

[6] A. Irshad, M. Sher, O. Nawaz, S. Chaudhry,I. Khan, and S. Kumari, "A secure andprovablemulti-server authenticatedkey agreementfor TMIS based on Amin et al. scheme", Multimed ToolsAppl., DOI 10.1007/s11042-016-3921-1, 2016.

[7] F.Wen,andX.Li,"Animproved dynamicID-based remote user authenticationwithkey agreement scheme," ComputersandElectrical Engineering, 38(2):381-387, 2012

[8] W.Juang,S.Chen,andH.Liaw, "Robust andefficientpassword authenticatedkey agreementusing smart cards,"IEEETrans.Ind. Electron.,vol.15,no.6,pp.2551-2556, Jun. 2008

[9] G.Yang,D.S. Wong,H.Wang and X. Deng, "Two-factor mutual authentication based onsmartcards and passwords," Journal of Computer and System Sciences, 74(7): 1160-1172, 2008

[10] M. Khan, S.Kim, and K. Alghathbar,"Cryptanalysis and security enhancementofamore efficientandsecure dynamicID-basedremote user authentication scheme. Computer Communications,34:305-309, 2011.