Secure Authentication Protocol for NFC Application using Pseudonyms

SINDHU D, SIVARANJANI R

SUJITHA R, THARANI T

UG Students,

Department of electronics and communication engineering

M. Kumarasamy College of Engineering

Karur, Tamilnadu

shrsindhu@gmail.com, sivaranjani9895@gmail.com,

sujitharajmohan@gmail.com, tharanithangaraj05@gmail.com

ABSTRACT

Authentication convention performs real part in the short separation correspondence operation for the Near Field Communication (NFC) strategy. Because of the common way of the saved correspondence framework there are few sorts of weakness. Starting late, a pen name NFC tradition (PBNFCP) set forward to survive the security pitfalls found in the current prohibitive insurance security tradition (CPPNFC). This venture advances advise PBNFCP and exhibits that notwithstanding it fails to keep the ensured security properties, for instance, pantomime assaults against a foe, who is a poisonous enlisted customer having a generous name relating private key. The proposed SEAP is reproduced for the formal security affirmation using the extensively recognized AVISPA (Automated Validation of Internet Security Protocols and Applications). SEAP is secure and productive when contrasted with the related existing verification conventions for NFC applications

I. INTRODUCTION

Since the fast improvement of short-range remote correspondence innovation, there is a developing interest to configuration secure and proficient portable applications, for example, benefit disclosure, e-payment, ticketing, and portable medicinal services frameworks, and so on, in the region of the shopper hardware for NFC. In the NFC environment, the Trusted Service Manager (TSM) is mindful to disperse client keys to the enlisted clients based upon the solicitations from the clients and it doesn't include in the confirmation procedure. The authentication convention includes just two gatherings, to be specific, an initiator client and target client. The initiator client creates a radio recurrence field what's more, begins the NFC interface. Subsequent to accepting correspondence signals, the objective client sends a reaction message to the initiator client through the radio recurrence field. After shared confirmation, both the initiator client and target client set up what's more, concede to a protected session key. Because of the mutual way of remote correspondence systems, there are a few sorts of security vulnerabilities in NFC environment including pantomime and man-in-the-center assaults. Besides, transmission limit of NFC innovation is constrained as its working recurrence is 13.56 MHz with transmission speed running from 106 Kbps to 424 Kbps up to 10 cm. Since the broadly utilization of cell phones, for example, advanced cells and individual portable workstations, in mix of NFC innovation, confirmation convention must guarantee high security alongside low calculation and correspondence costs.

A. Related works

An open key foundation is utilized for the productive key administration and repudiation among hubs, such as initiator and target clients. In this situation, a foe could track the client's exercises by following its open key, and therefore, the client's security might be broken. In request to beat these downsides, the nom de plume is utilized as a part of numerous confirmation conventions incorporate NFC

and vehicular specially appointed systems (VANETs) another restrictive protection safeguarding security convention (CPPNFC) to ensure the client's protection. However, CPPNFC neglects to keep the pantomime assaults, and further proposed a pseudonym NFC convention (PBNFCP) to withstand the security downsides found in CPPNFC with a minimal computational cost increment. This paper proposes another protected and effective confirmation convention (SEAP) for NFC applications utilizing the new characterized life time based pseudonyms to withstand the PBNFCP.

B. Commitments

The commitments of the paper are recorded beneath:

(i) This paper examines and demonstrates that the as of late proposed PBNFCP neglects to give the guaranteed security properties, for example, pantomime assaults against a vindictive enlisted client being an assailant.

(ii) In this paper, another safe and proficient validation convention (SEAP) is exhibited for the NFC applications utilizing the life time-based pseudonyms. The proposed alias private key combine in SEAP is substantial inside its lifetime as it were. In this way, regardless of the possibility that a pseudonym private key match is out of the blue uncovered to a foe, he/she can utilize it inside its expiry time for the relating client as it were. Accordingly, the weakness for this situation is constrained to the comparing client just, though in PBNFCP, CPPNFC, and it causes to the pantomime assaults to any authentic client in the framework when the personality of that client is known to the foe. Besides, the span of the proposed alias SEAP is altogether lessened.

(iii) The thorough casual security investigation shows that SEAP is secure against conceivable surely understood assaults including the impersonation and man-in-the-middle attacks. Moreover, the reproduction comes about for the formal security check utilizing the broadly acknowledged AVISPA instrument indicates that SEAP is secure against the detached and dynamic assaults.

(iv) SEAP fundamentally lessens the calculation and correspondence costs, furthermore gives more security functionalities when contrasted with the related existing conventions.

(v) Due to productivity and more security functionalities, SEAP is extremely appropriate for the short-extend remote Correspondence applications, for example, benefit revelation, e-payment, ticketing, and Portable medicinal services frameworks, and so on, in the zone of the shopper electronic gadgets in the NFC environment.

C. Association of the paper

Whatever is left of the paper is outlined as takes after. In Section II, a brief survey of SEAP convention is given. In Section III, the security analyses of SEAP convention are talked about. The recreation of SEAP for the formal security check utilizing the broadly acknowledged AVISPA device is given in Section IV. The execution of SEAP with related existing conventions and the result is thought about in Section V.

II. THE PROPOSED SEAP PROTOCOL

In this segment, another protected and effective pen name security convention (SEAP) is proposed to withstand the security pitfalls found in different conventions. The proposed SEAP comprises of two stages, in particular, pseudonym stage and session key foundation stage.

A. Pseudonym request phase

A client *X* solicitations the TSM for the pseudonyms verify and set up a session with different clients. All together to beat the security disadvantages found in various conventions, the TSM creates *n* pseudonyms private key pairs, say (A^j_X, e^j_X) utilizing the elliptic bend cryptography (ECC)base EI-Gammal sort signature as follows.

The TSM first chooses n random numbers b^j_X ,j=1,….,n, and computes $A^j_X=\{B^j_X||Enc(e_{TSM}$,$\{ID_X$,$b^j_X\})||$ $ID_{TSM}||YZ^j_X\}$, $e^j_X=b^j_X+h(ID_X,ID_{TSM},A^j_X)e_{TSM}$

Where $B^j_X=b^j_xI$ is jth public key. The TSM sends the n pseudonym and private key pairs (A^j_X , e^j_X) to the user *X* via a secure channel what's more, stores the character An ID_X and relating pseudonyms A^j_X's of An in its database until lapse of the sets. It is watched that regardless of the possibility that a pseudonym private key match is startlingly uncovered to a foe, he/she can as it were utilize it inside its expiry time for the benefit of comparing client. This suggests

plausibility of weakness is restricted to the relating client just, though in PBNFCP and other conventions, it causes pantomime assaults to any true blue enrolled client.

B. Session key establishment phase

In this stage, the procedure of verification and key agreement between an initiator client *X* and an objective client *Y* of SEAP is talked about. So as to set up a session key

AB= AB_X= AB_Y, X and *Y* need to execute.

1)X randomly picks a pseudonym and private key pair(A^j_X,e^j_X), and sends the request $N_1=\{A^j_X\}$ to Y via a public channel

III. SECURITY ANALYSIS OF SEAP PROTOCOL

In this area, SEAP is altogether dissected and appeared that it is secure against the well known assaults including the man-in-the-middle assault.

A. Impersonation attack

During calculation of private key, SEAP processes it utilizing three fields as a part of hash work, that is, e^j_X as b^j_X+h(ID_x,ID_{TSM}, A^j_X)eTSM. Consequently, the pen name private key combine (A^j_X,e^j_X) turns into an El-Gamal sort ECC-construct signature with respect to the character An ID_X of client X created by the TSM's private key $e_{TSM.}$ Expect that an aggressor *D* is an enrolled client with a substantial pseudonym and private key combine (A^l_d , e^l_d), and clients *X* and *Y* are two communicating parties. *D* neglects to confirm at both X and Y by propelling the pantomime assault.

B.Secure mutual authentication

Since (A^j_X,e^j_X) is the El-Gamal sort ECC-based mark on ID_X, it is computationally hard for an enemy *D* to create such a substantial combine because of the trouble of comprehending elliptic bend discrete logarithm issue (ECDLP). In this way, *D* does not have any capacity to register the substantial $MacTag_X$ to be validated by B and $MacTag_Y$ to be confirmed by X. This suggests SEAP counteracts unapproved alterations, furthermore, along these lines, the clients X and Y commonly verify each other by approving $MacTag_Y$ and $MacTag_X$, individually. Subsequently, SEAP gives secure shared validation.

C. Client secrecy

It guarantees that an enemy *D* can't follow the client exercises by catching the transmitted messages. *D* has full control over the correspondence because of remote system utilized as a part of NFC applications. Expect that *D* captures every one of the messages $N_1=\{A^j_x\}$, $N_2=\{PQ,A^i_Q\}$, $N_3=\{PX, MacTag_X\}$ and $N_4=\{MacTag_Y\}$ transmitted between the clients X and Y. The client character is included in the relating pseudonyms A^j_X, A^i_Y , which are then encoded by the TSM's private key. Therefore, aside from the TSM, no foe can process the genuine character of a client from given alias no foe can check whether the pseudonym to the given client character due to the trouble of fathoming ECDLP. Then again, no foe can recover the genuine personality from $MacTag_X$ and $MacTag_Y$ due to the restricted crash resistance hash work property. In this way, the enemy can't follow the first client personality from the blocked correspondences. Accordingly, SEAP gives the client namelessness property.

D.Replay assault

From the above contentions, no enemy can register substantial verification and affirmation messages to be confirmed by clients X and Y utilizing blocked messages as SEAP forestalls unapproved changes. No enemy can then effectively set up the session by replaying caught messages without relating substantial nom de plume private key match. As producing legitimate pseudonym private key combine is computationally difficult issue because of fathoming ECDLP, the foe can't dispatch the replay assault. Subsequently, SEAP is secure against the replay assault.

D.Man-in-the-center assault

In this assault, an enemy tries to imitate the lawful clients by catching the messages between imparting clients utilizing accessible open data. Be that as it may, from above dialog, SEAP averts pantomime assaults and gives secure shared confirmation between two conveying parties. Thus, SEAP is secure against this assault.

E. Adjustment assault

A foe does not have any capacity to process substantial $MacTag_X$= h(G_X,ID_X,ID_Y,P_X,P_Y) be confirmed by Y what's more $MacTag_Y$= h(TG_Y,ID_Y,ID_X,P_Y,P_X) to be verified by X because of

the trouble of creating El-Gammal sort ECC based signature on given personality. Accordingly, SEAP effectively keeps the unapproved alterations.

IV. SIMULATION FOR FORMAL SECURITY VERIFICATION UTILIZING AVISPA TOOL

In this segment, SEAP is reproduced utilizing the widely accepted AVISPA apparatus to demonstrate that SEAP is secure.

A. Outline of AVISPA

AVISPA is a push-catch apparatus for computerized approval of Web security-touchy conventions and applications, which formally confirms whether a security convention is protected or perilous. Different fundamental sorts bolstered by HLPSL are as per the following operator, symmetric key, public key, hash_func, nat, and content speak to the important names, mystery enters in a symmetric key cryptosystem, open keys in an open key cryptosystem, cryptographic hash work, common numbers in non-message settings, and a nonce. Take note of that if a given open (individually private) key ku, its opposite private (individually open) key is signified by inv_ku, separately. What's more, if N is a sort content (crisp), N' is a new esteem which an interloper can't get it.

B.Investigation of results

The generally acknowledged OFMC and CL-AtSe back ends are decided for the execution tests and a limited number of sessions display checking. For replay assault insurance, these back ends check whether the genuine operators (clients) can execute the predetermined convention by method for playing out a inquiry of a uninvolved interloper. For the Dolev-Yao check, the backends check if there is any man-in-the-center assault conceivable by the gatecrasher. The proposed SEAP is reproduced utilizing SPAN (Security Protocol Animator for AVISPA) for OFMC and CL-AtSe. The simulation comes about for the formal security confirmation of SEAP guarantee that SEAP is secure against the replay and man-in-the-middle assaults. The outline of the outcomes reported under OFMC and CL-AtSe back ends reports that SEAP is protected.

V. CONCLUSION

The late proposed convention is initially broke down and afterward demonstrated that it is helpless against two sorts of security. SEAP: Secure and Efficient Authentication Protocol for NFC Applications Using Pseudonyms 37 pantomime assaults. A novel secure and effective verification convention (SEAP) for NFC applications is proposed utilizing the lifetime-based pseudonym essentially low calculation and correspondence costs as contrasted with existing related verification conventions. Through the thorough security examination, it is demonstrated that SEAP is secure against conceivable known assaults including the impersonation assaults found in convention. In expansion, the reproduction comes about for the formal security confirmation utilizing the broadly acknowledged AVISPA apparatus plainly demonstrates that the proposed SEAP is secure. In this manner, SEAP gives high security alongside low calculation and correspondence.

REFERENCES

[1] Gartner, "Market Insight: The Outlook on Mobile Payment," *Market Analysis and Statistics*, May 2010.

[2] Juniper Research, "NFC Mobile Payments & Retail Marketing-Business Models & Forecasts 2012-2017," May 2012.

[3] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953-1966, Jun. 2015.

[4] R. Want, "Near field communication," *IEEE Pervasive Comput.*, vol.10, no.3, pp. 4 - 7, July. 2011.

[5] V. Patil, N. Varma, S. Vinchurkar, and B. Patil, "NFC based health monitoring and controlling system," *in Proc. IEEE Global Conference on Wireless Computing and Networking*, Lonavala, India, pp. 133-137, Dec. 2014.

[6] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 2259-2294, Aug. 2013.

[7] W. Lumpkins and M. Joyce, "Near-Field Communication: It Pays: Mobile payment systems explained and explored," *IEEE Consume. Electron. Mag.*, vol.4, no.2, pp.49-53, Apr. 2015.

[8] F. Michahelles, F. Thiesse, A. Schmidt, and J. R. Williams, "Pervasive RFID and near field communication technology," *IEEE Pervasive Compute.*, vol. 6, no. 3, pp. 94-95, July. 2007.

[9] V. Coskun, K. Ok, and B. Ozdenizci, *Near Field Communication (NFC): From Theory to Practice*, London: Wiley. ISBN: 978-1-11997109-2, Feb. 2012.

[10] J. Ondrus and Y. Pigneur, "An assessment of NFC for future mobile payment systems," *in Proc. International Conference on theManagement of Mobile Business*, Toronto, Canada, pp. 43-43, July 2007.

[11] ISO/IEC 15946-1:2008, "Information technology - Security methods-Cryptographic methods based on elliptic curves - Part 1: General," Apr.2008.

[12] ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems - NFC Security - Part 1:NFC-SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.

[13] ISO/IEC 13157-2:2010, "Information technology Telecommunications And information exchange between systems - NFC Security - Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[14] S. Kannadhasan, M. Isaivani, and G. Karthikeyan, "A Novel Approach Privacy Security Protocol Based SUPM Method in Near Field Communication Technology," *in Proc. Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Kumaracoil, India, vol. 324, pp. 633-643, Nov. 2014.

[15] J. H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," *Math. Comput. Model.*, vol. 55, no. 1, pp. 170-187, Jan. 2012.

[16] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," *in Proc. ACM International Workshop on Vehicular Ad hoc Networks*, Montréal, QC,Canada, pp. 19-28, Sept. 2007.

[17] H. Eun, H. Lee, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," *IEEE Trans. Consumer Electron.*, vol.59, no. 1, pp.153-160, Apr. 2013.

[18] D. He, N. Kumar, and J. H. Lee, "Secure pseudonym-based near field communication protocol for the consumer internet of things," *IEEE Trans. Consumer Electron.*, vol. 61, no. 1, pp. 56-62, Mar. 2015.

[19] V. Odelu, A. K. Das, and A. Goswami, "A secure and efficient ECC based user anonymity preserving single sign-on scheme for distributed computer networks," *Secur. Comm. Netw.*, vol. 8, no. 9, pp. 1732-1751, Jun. 2015.

[20] D. Basin, S. Mödersheim, and V. Luca, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3 pp. 181-208, Jun. 2005.

[21] A. Armando et al., "The AVISPA Tool for the Automated Validation of Internet Security protocols and Applications," *in Proc. International Conference on Computer Aided Verification*, Scotland, UK, LNCS, vol. 3576, pp. 281-285, July 2005.

[22] C. Lv, M. Ma, H. Li, J. Ma, and Y. Zhang, "An novel three-party authentication key exchange protocol using one-time key," *J. Netw.Comput. Appl.*, vol. 36, no. 1, pp. 498-503, Jan. 2013.

[23] A. K. Das, "A Secure and Efficient User Anonymity-Preserving Three-Factor Authentication Protocol for Large-Scale Distributed Wireless Sensor Networks," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1377-1404, Jun. 2015.

[24] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," accepted for publication in Int. J. Commun. Syst., Jan. 2015.

[25]. V.Kavitha, C.Gayathri, “A Survey on Detection Methods for Network Layer Attacks in WMN's”, International Journal of Applied Engineering Research, Vol.10, Issue 1, pp.744-748, 2015.

[26] S.Palanivel Rajan, S.Vijayprasath, “Performance analysis on web based Traffic control for DDoS attacks”, International Journal of Engineering Research and General Science, Vol.3, No.1, pp. 477-482, 2015.

[27]. V.Kavitha, C.Gayathri, “An Analysis on Routing and Issues in Network Layer in WMN's”, International Journal of Scientific and Engineering Research, Vol. 6, Issue 4, pp.120-125, 2015.

[28]B.Neeththi Aadithiya, P.T.Sivagurunathan “A Survey on Geographic Routing Protocols for MANETs” International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.1 (2015) pp. 717-722.