Secure and Efficient Authentication Protocol using Pseudonym

Sivaranjani R, Sujitha R, Sindhu D, Tharani T*

Department of Electronics and Communication Engineering, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India.

***Corresponding author: E-Mail: tharanithangaraj05@gmail.com**

ABSTRACT

Authentication Protocol assumes a vital part in the short range remote interchanges for the Near Field Communication (NFC) innovation. Its operating frequency is 13.56 MHz with the transmission speed range from 106 Kbps to 424 Kbps. Because of the mutual nature of remote communication systems, there are a few sorts of security vulnerabilities. Starting late, a life time based NFC protocol (PBNFCP) has been proposed to withstand the security pitfalls found in the restrictive security insurance security tradition. In any case, this project facilitate examines PBNFCP and demonstrates that regardless it neglects to keep the guaranteed security properties, for example, impersonation attacks against an adversary, who is a noxious enrolled client having a substantial name relating private key. The proposed SEAP is reproduced for the formal security affirmation using the comprehensively recognized AVISPA (Automated Validation of Internet Security Protocols and Applications). SEAP is secure and efficient as compared to the related existing authentication protocols for NFC applications.

KEY WORDS: AVISPA (Automated Validation of Internet Security Protocols and Applications), SEAP.

1. 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 (Agnus Swarnanisha Lakshmi and Palanivel Rajan, 2016). 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. Ensuing to tolerating correspondence flags, the target customer sends a response message to the initiator customer through the radio repeat field. After shared confirmation, both the initiator client and target client set up what's more, concede to a protected session key (Dhivya and Kavitha, 2014). 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 (Kavitha and Gayathri, 2015). 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 (Kavitha and Palanisamy, 2013). 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 (Mohanapriya and Vadivel, 2013).

2. 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 (Palanivel Rajan, 2015).

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 (Palanivel Rajan and Poovizhi, 2016). This paper proposes another protected and effective confirmation convention (SEAP) for NFC applications utilizing the new characterized life time based pseudonymsto withstand the PBNFCP.

Commitments: The commitments of the paper are recorded beneath:

- In this paper, another safe and proficient validation convention (SEAP) is exhibited for the NFC applications utilizing the life time-based pseudonyms (Palanivel Rajan, 2013). 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.

- 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
- 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 (Palanivel Rajan, 2012).

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 (Palanivel Rajan, 2014). The proposed SEAP comprises of two stages, in particular, pseudonym stage and session key foundation stage (Palanivel Rajan and Vijayprasath, 2015).

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 $B^j_X=b^j_x I$ 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.

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.

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 (Shriram Vasudevan and Vivek, 2015).

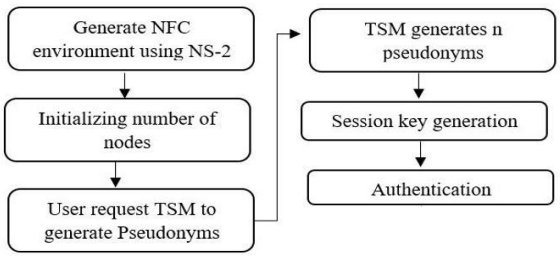

Figure.1. Procedure of verification and key agreement between an initiator client and an objective client

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.

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 (Shriram Vasudevan and Vivek, 2015). *D* neglects to confirm at both X and Y by propelling the pantomime assault.

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 MacTagY 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.

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 aliasno foe can check whether the pseudonym to the given client character due to the trouble of fathoming ECDLP (Sridevi and Prasannavenkatesan, 2016). 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.

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 (Sundaravadivu and Bharathi, 2013). 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 (Palanivel Rajan, 2016).

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 (Sukanesh, 2010). Thus, SEAP is secure against this assault.

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.

Advanced Encrpytion Standard for Nfc: The more noticeable and for the most part grasped symmetric encryption count inclined to be encountered nowadays is the Advanced Encryption Standard (AES). It is found no under six circumstances speedier than triple DES. AES is a square figure with a piece length of 128 bits. AES considers three particular key lengths: 128, 192, or 256 bits. A substantial segment of our examination will expect that the key length is 128 bits. Encryption involves 10 rounds of dealing with for 128-piece keys, 12 rounds for 192-piece keys, and 14 rounds for 256-piece keys. Except for the last round for each circumstance, each other round is unclear. Each round of taking care of fuses one single-byte based substitution step, a line smart change step, a segment keen mixing step, and the extension of the round key (Vasudevan, 2015). These four phases are executed is particular for encryption and unscrambling. Encryption writing computer programs is implementable in C and Java. AES is an iterative rather than Feistel figure. It relies on upon 'substitution–permutation orchestrate'. It contains a movement of associated operations, some of which incorporate supplanting commitments by specific yields (substitutions) and others incorporate revamping bits around (changes). Abnormally, AES plays out each one of its counts on bytes rather than bits. Thus, AES treats the 128 bits of a plaintext frustrate as 16 bytes. These 16 bytes are sorted out in four portions and four sections for get ready as a grid.

Each of the four sections of the lattice is moved to the other side. Any segments that 'tumble off' are re-inserted on the right half of line. Move is done as takes after − To start with segment is not moved. Second line is moved one (byte) position to the other side. Third line is moved two positions to the other side. Fourth segment is moved three positions to the other side. The result is another cross section involving a comparative 16 bytes yet moved in regards to each other. Each portion of four bytes is right now changed using a one of a kind logical limit. This limit takes as information the four bytes of one area and yields four absolutely new bytes, which supplant the primary section (Vivek and Audithan, 2014). The result is another new system including 16 new bytes (Shriram Vasudevan and Vivek, 2015). It should be seen that this movement is not performed in the last round. The 16 bytes of the cross section are by and by considered as 128 bits and are XORed to the 128 bits of the round key. In case this is the last round then the yield is the figure content. Something else, the consequent 128 bits are deciphered as 16 bytes and we begin another similar round.

In present day cryptography, AES is by and large gotten and maintained in both hardware and programming. Till date, no practical cryptanalytic attacks against AES have been found. Likewise, AES has worked in flexibility of key length, which allows a level of 'future-fixing' against progress in the ability to perform intensive key chases (Vivek and Palanivel Rajan, 2016). In any case, likewise concerning DES, the AES security is ensured just if it is precisely completed and extraordinary key organization is used.

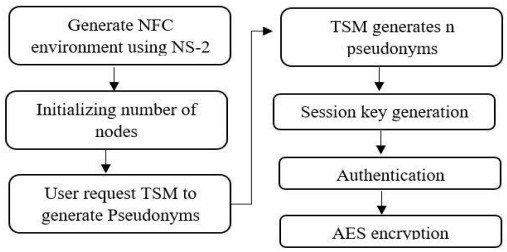

Figure.2. Process flow for AES Encryption

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.

Outline of AVISPA: AVISPA is a push-get contraption for electronic endorsement of Web security-delicate traditions and applications, which formally affirms whether a security tradition is ensured or dangerous. 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.

3. INVESTIGATION OF RESULTS

The by and large recognized OFMC and CL-AtSe back closures are chosen for the execution tests and a set number of sessions show checking. For replay ambush protection, these back closures check whether the certifiable administrators (customers) can execute the foreordained tradition by strategy for playing out a request of a uninvolved gatecrasher. For the Dolev-Yao check, the back finishes check if there is any man-in-the-inside strike possible by the interloper. 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.

4. 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

Agnus Swarnanisha Lakshmi, Palanivel Rajan S, Scheduled H and X Medicine Dispenser PoC Design, Journal of Chemical and Pharmaceutical Sciences, 8, 2016, 1-4.

Dhivya R, Kavitha V, Secured Client Cache Sustain for Maintaining Consistency in MANET's, International Journal of Research in Engineering and Technology, 3(7), 2014, 1-6.

Kavitha V, Gayathri C, An Analysis on Routing and Issues in Network Layer in WMN's, International Journal of Scientific and Engineering Research, 6 (4), 2015, 120-125.

Kavitha V, Palanisamy V, Load Balanced Deflection Routing and Priority Scheduling in OBS Networks, International Review on Computers and Software, 8 (7), 2013, 1603-1612.

Kavitha V, Palanisamy V, New Burst Assembly and Scheduling T technique for Optical Burst Switching Networks, Journal of Computer Science, 9 (8), 2013, 1030-1040.

Kavitha V, Palanisamy V, Simultaneous Multi-path Transmission for Burst Loss Recovery in Optical Burst Switching Networks, European Journal of Scientific Research, 87 (3), 2012, 412-416.

Mohanapriya S, Vadivel M, Automatic retrieval of MRI brain image using multi queries system, International Conference on Information Communication and Embedded Systems (ICICES), 2013, 1099-1103.

Palanivel Rajan S, A Survey on Detecting Methods of Driver Drowsiness, International Journal of Innovations in Engineering and Management, 4 (1), 2015, 1-5.

Palanivel Rajan S, Diagnosis of Cardiovascular Diseases using Retinal Images through Vessel Segmentation Graph,Current Medical Imaging Reviews, 13 (2), 2017.

Palanivel Rajan S, Experimental Explorations on EOG Signal Processing for Real Time Applications in LabVIEW, IEEE Digital Library Xplore, 2012.

Palanivel Rajan S, Poovizhi M, Design of Patch Antenna Array for Radar Communication, Journal of Chemical and Pharmaceutical Sciences, 8, 2016, 38-40.

Palanivel Rajan S, Sukanesh R, Ramprasad A, Jayakumar M, A Comprehensive Analysis of Wireless Mobile Based Tele-Monitoring System for Myocardial Malfunctioning, International Journal of Computer Sciences issues, 9 (3), 2012, 578- 582.

Palanivel Rajan S, Sukanesh R, Vijayprasath S, Assessment of Relationship between Heart Rate Variability and Drowsiness of Post-Operative Patients in Driving Conditions, Health MED Journal, 8 (2), 2014, 211-221.

Palanivel Rajan S, Vijayprasath S, Performance analysis on web based Traffic control for DDoS attacks, International Journal of Engineering Research and General Science, 3 (1), 2015, 477-482.

Palanivel Rajan S, Vijayprasath S, Sukanesh R, Certain Investigations on Eye State Analysis for the Development of a Non-Intrusive Fatigue Detection System, European Journal of Scientific Research, 93 (3), 2012, 342-350.

Palanivel Rajan S, Visual and tag-based social image search based on hyper graph ranking method, IEEE Digital Library Xplore, 2015.

Palanivel Rajan S, Vivek C, Paranthaman M, Feasibility Analysis of Portable Electroencephalography Based Abnormal Fatigue Detection and Tele-Surveillance System, International Journal of Computer Science and Information Security, 14 (8), 2016, 711-722.

Palanivel Rajan S, Performance Evaluation on Segmentation of Dental CT Images for Individual Recognition, International Journal of Advances in Computer and Electronics Engineering, 1 (2), 2016, 17-20.

Paranthaman M, Vijayprasath S, Palanivel Rajan S, Design of a Frequency Tunable Patch Antenna using HFSS, International Journal of Advanced Research Trends in Engineering and Technology, 3 (7), 2016, 69-72.

Shriram Vasudevan K, Vivek C, An Intelligent Attempt to Export Files in to Cloud in Handheld Devices through Gesture Recognition, Indian Journal of Science and Technology, 8, 2015, 1-8.

Sridevi A, Prasannavenkatesan G.K.D, A Survey of PAPR Reduction in OFDM Signals, Journal of Advances in Chemistry, 12 (23), 2016, 5478-5483.

Sukanesh R, Palanivel Rajan S, Vijayprasath S, Janardhana Prabhu S, Subathra P, GSM-based ECG Tele-alert System, International Journal of Computer Science and Application Issue, 2010, 112-116.

Sundaravadivu K and Bharathi S, STBC codes for generalized spatial modulation in MIMO systems, IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), Tirunelveli, 2013, 486-490.

Vasudevan SK, Vivek C, Srivathsan S, An Intelligent Boxing Application through Augmented Reality for two users Human Computer Interaction Attempt, Indian Journal of Science and Technology, 8 (34), 2015, 1-7.

Vivek C, Audithan S, A Statistical Approach of Text on Based Texture Classification Using LP boosting Classifier, Research Journal of Applied Sciences Engineering and Technology, 7 (19), 2014, 4088-4094.

Vivek C, Audithan S, A Novelty Approach of Spatial Co-Occurrence and Discrete Shearlet Transform Based Texture Classification Using LP-Boosting Classifier, Journal of Computer Science, 10 (5), 2014, 783-793.

Vivek C, Audithan S, Rotation Scale Invariant Texture Classification for a Computational Engine, Research Journal of Applied Sciences Engineering and Technology, 8 (13), 2014, 1572-1577.

Vivek C, Palanivel Rajan S, Design of Data Aware Low Power Area Efficient Data paths for Processing Elements in a Reconfigurable System, International Journal of Computer Science and Information Security, 14 (9), 2016, 711-722.