Middle-East Journal of Scientific Research 20 (6): 756-757, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.20.06.11391

New Forward-Secure Digital Signature Scheme

K. Karthick, P. Jennifer and A. Muthukumaravel

Department of MCA, Bharath University,
Selaiyur, Chennai, 73, Tamil Nadu, India

Abstract: In this paper, the widely used ECC digital signature scheme – ECDSA is advanced and a new forward-secure digital signature scheme is proposed in order to reform the n this limitations of ECDSA. In the new scheme, although the digital signature's private key is under the control of a one-way function and continually changed in different durations with time goes by, its public key remains the same. The attacker could not fake the older signature even if the private key is leaked out in some period of time. In this way this scheme makes sure of the security of signature of former phases. The validity of the new scheme is proved and the security is analyzed in the paper. The widely used public key digital signature scheme is designed on the *NP* problem in mathematics. The ECC Digital Signature constructs discrete logarithm problem by using the Abel additive group composed of the points on elliptic curve. With the development of the computer sciences and the communication business, digital signature becomes one of the most important means to guarantee the security of communication. But in reality, the signature private key may be leaked out through the secret leaks of system or factitious factors, so the signature may be faked, which become a difficult part of security problem. This article based on non-supersingular elliptic curve over finite field *n GF* with eigenvalue *n* 2 [4], advances a kind of forward-secure digital signature scheme. javac. The Java compiler produces a file called a. class file, which contains the byte code. The. Class file is then loaded across the network or loaded locally on your machine into the execution environment is the Java virtual machine, which interprets and executes the byte code.

Key words: ECC digital signature scheme % Although the digital signature's private key % Security of communication

INTRODUTION

Proposed System:

- The biggest advantage to public-key cryptography is the individuals do not need to agree on a single key. Anyone can know anyone's public key and only the key's owner knows the private key [1-7].
- EC operations are generally faster than DL, IF counterparts at comparable key sizes. Key pair generation is much faster than for IF.
- EC Discrete Logarithm Problem is very different than DL, IF hard problems.EC data are shorter than DL, IF counterparts.
- Intermediate values are shorter. Signatures with appendix are same size as for DL, shorter than IF.

System Implimentation: Implementation is the stage in the project where the theoretical design is turned Into a working system and is giving confidence on the new system for the users, which it will work efficiently and effectively [8]. It involves careful planning, investigation of the current System and its constraints on implementation, design of methods to achieve the change over, an evaluation, of change over methods. Apart from planning major task of preparing the implementation are education and training of users [9]. The more complex system being implemented, the more involved will be the system analysis and the design effort required just for implementation.

An implementation co-ordination committee based on policies of individual organization has been appointed. The implementation process begins with preparing a plan

Corresponding Author: K. Karthick, Department of MCA, Bharath University, Selaiyur, Chennai, 73, Tamil Nadu, India.

for the implementation of the system. According to this plan, the activities are to be carried out, discussions made regarding the equipment and resources and the additional equipment has to be acquired to implement the new system. Implementation is the final and important phase, the most critical stage in achieving a successful new system and in giving the users confidence. That the new system will work be effective [10]. The system can be implemented only after through testing is done and if it found to working according to the specification. This method also offers the greatest security since the old system can take over if the errors are found or inability to handle certain type of transactions while using the new system.

Personal and confidential information is stored on a wide variety of enterprise data resources. To secure and protect this data, technology must adapt to mitigate the threats and risks arising from the trend toward dynamic enterprises, adaptive data centers and on-demand resource allocation. Applications and services are becoming mobile across multiple resources, sometimes in a dynamically allocated way, necessitating the migration of sensitive and private data [11]. We propose a policy-driven data-protection system to address the inadequacies of current technological solutions in preserving the confidentiality and privacy of data while it migrates between platforms. More specifically, we describe our solution for securing credential migration that we're developing for productization.

CONCLUSION

Forward-secure digital signature scheme which is based on elliptic curve cryptography digital signature scheme ECDSA. Meanwhile the new scheme's security and validity is proved. Because the new scheme is target on to ensure that, the attacker still could not fake the signature of the past time even if the private key in signature is leaked out in some period of time, it insure the signature's forward security and damage caused by leaked out key can be limited and controlled.

Future Enhancement: The project A New Forward Digital Signature |Scheme is to maintain the work detail, Of the employees,designation, department,and client and also details of the project and the assignment of the project.

Each employee as the login id so that on giving that particular id the superiors can work status of that particular employee..

In future, I would like to apply additional features like to allow the employee to view their profile from anywhere of the world with help of their employee to view their profile from anywhere of the world with the help of their employee id. The services will be provided by the adiminstrator as a server.

REFERENCES

1. Vanstone, S., 1992. Reponses to NIST's proposal. Communications of the ACM, 35: 50-52.
2. Bellare, M. and S.K. Miner, 1999. A forward-secure digital signature scheme. In: Proc of the CRYPTO'99. Berlin: Springer-Verlag, pp: 431~448.
3. Bellare, M., 1999. Practice -Oriented provable-security. In: Damgard I, ed. Advances in Cryptology Eurocrypt'99. LNCS 1561, Berlin: Springer-Verlag, pp: 221-231.
4. Micali, S. and L. Reyzin, 1999. Improving the exact security of Fiat-Shamir signature schemes. In R. Baumgart, ed., Secure Networking-CQRE [Secure]' 99, volume 1740 of Lecture Notes in Computer Science, pages 167–182, Springer-Verlag,. CrossRef.
5. Ohta, K. and T. Okamoto, 1988. A Modification of the Fiat-Shamir Scheme, Advances in Cryptology-Crypto 88 Proceedings, Lecture Notes in Computer Science, S. Goldwasser ed., Springer-Verlag, Cross Ref, 403: 232-243.
6. Pointcheval, D. and J. Stern, 1996. Security proofs for signature schemes, Advances in Cryptology-Eurocrypt 96 Proceedings, Lecture Notes in Computer Science U. Maurer ed., Springer-Verlag, pp: 1070.
7. Kerana Hanirex, D. and K.P. Kaliyamurthie, 2013. Multi-classification approach for detecting thyroid attacks, International Journal of Pharma and Bio Sciences, 4(3): B1246-B1251.
8. Khanaa, V., K. Mohanta and T. Saravanan, 2013. Comparative study of uwb communications over fiber using direct and external modulations, Indian Journal of Science and Technology, 6(suppl 6): 4845-4847.
9. Kumar Giri, R. and M. Saikia, 2013. Multipath routing for admission control and load balancing in wireless mesh networks, International Review on Computers and Software, 8(3): 779- 785.
10. Kumaravel, A. and K. Rangarajan, 2013. Routing alogrithm over semi-regular tessellations, 2013 IEEE Conference on Information and Communication Technologies, ICT 2013.
11. Kumaravel, A. and K. Rangarajan, 2013. Algorithm for automaton specification for exploring dynamic labyrinths, Indian Journal of Science and Technology, 6(suppl 6).