International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

ENHACE SECURITY OF DUAL SIGNATURE BY FUZZY CONTROLLER

Seyed Hasan Mortazavi Zarch[1,*] ,Prof.P.S.Avadhani[2] , Madihesadat Yazdanivaghef[3]
PhD Scholar, department of CS&SE Andhra University,India[1]
Vice Principal, Andhra University College of Engineering,India[2]
Master of Science Computer study at Andhra University,India[3]

Abstract

In this paper we use fuzzy controller for enhancing security of Dual signature, this technique that can be applied to prove security from static assumptions for new signature by Fuzzy Controller. Our work prevent of Desmedt and Odlyzko's attack (chosen-cipher text attack) on RSA encryptions and chosen-message attack on RSA Signatures. When hacker wants to attack on RSA encryption with chosen text attack cannot access to plain text because plaintext converted to fuzzy data by fuzzy controller. The result of this procedure is to raise dual Signature security.

Key word: RSA, Dual Signature, fuzzy controller, SET.

1. Introduction

A significant novation introduced in SET (**Secure Electronic Transaction**) is the dual signature. The goal of the dual signature (DS) is the same as the standard E-signature to assurance the integrity and authentication of information or data.

In Dual Signature used public-key cryptosystem (RSA). RSA can be used for both encryption and signature. Although RSA is used for encryption but attacks such as chosen-cipher text attack against plain RSA encryption and chosen-message attack on **RSA Signatures** take place. To this end, we began to feel secure dual signature. And fuzzy controller is designed for the dual signature.

Secure electronic Transaction (SET) was a communications protocol for safe or securing Master or credit card transactions over insecure internet. Secure electronic Transaction (SET) was not itself a payment, but rather a set of security protocols and formats that active user to engage the existing master or credit card payment infrastructure on a computer networks in a secure fashion. [1].

Fuzzy logic is a branch of applied artificial intelligence for the first time in the 80th By Professor Lotfi Zadeh was submitted. Based fuzzy logic to prove the convergence of higher mathematics which deals with system response this is out of the question. This phase of the design engineer to work in their system looks to see a black box and Designed to work only with knowing various inputs and output of the system is to correct errors. In all the above values is qualitatively (Low, very low, high, etc.) Controller logic one or logic zero is not so black and white .The controller is able to control and predict the failure behavior of the system for all values. In many applications, e.g., space projects exact system of equations is impossible or very difficult. Fuzzy enabled the design engineers that without a system of equations to be able to control it. The fuzzy super-fast microprocessor applications requiring Very fast also destroyed and since the controller does not need to solve complex equations the simpler algorithms and high-speed error will be corrected [2].

2. Dual signature

The goal of the dual signature (DS) is that the same as the standard electronic signature to ensure the authentication and integrity of information or data. It links two messages that are intended for two various receivers. Hereon, the customer or purchaser wants to dispatch the order information (OI) to the merchant or businessman and the payment information (PI) to the bank. The businessman or merchant is not incumbent to know the customer's Master or credit card number, and the bank doesn't need knowing the details of the customer's order. The link doesn't need so that the purchaser or customer can prove that the payment is intended for this order [1].Figure 1.

ISSN:2319-7900

$$DS = E_{KR_c}[H(H(PI) \| H(OI))]$$

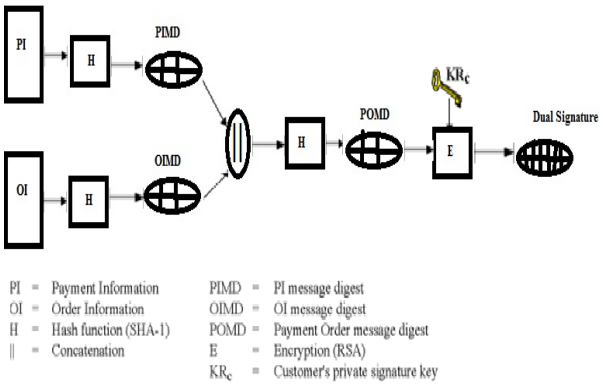

Fig 1. Dual Signature

Above figure.1 shows the model of dual signature [1]. When the dual signature is constructed, it gets the hash of the concatenated hashes of Order Information (OI) and Payment Information (PI) as inputs. The dual signature is the encrypted message digest (MD) with the customer's secret key of the connected message digest's (MD) of Payment Information (PI) and Order Information (OI). The dual signature (DS) is dispatched to both the businessman or merchant and the bank. The protocol sets for the businessman or merchant to see the message digest (MD) of the Payment Information (PI) without seeing the Payment Information (PI) itself, and the bank sees the message digest (MD) of the Order Information (OI) but not the Order Information (OI) itself. The dual signature (DS) may be verified using the message digest (MD) of the Order Information (OI) or Payment Information (PI). It doesn't need the Order Information (OI) or Payment Information (PI) itself. Its message digest (MD) does not disclose the content of the Order Information (OI) or Payment Information (PI), and so privacy is protected [1].

3. Vulnerability of dual signature

RSA was invented in 1977 by Rivest, Shamir and Adleman [4], and is now the most widely used public-key cryptosystem. RSA can be used for both encryption and signature. A chosen-cipher text attack against plain RSA encryption was explained at Crypto '85 by Desmedt and Odlyzko [3]. Two attacks took place on RSA:

- **Attack on RSA Encryption**

In [5], Desmedt and Odlyzko explain a chosen-ciphertext attack against plain RSA encryption.

- **Attack on RSA Signatures**

The previously described attack against RSA encryption can be easily adapted to RSA signatures to provide an existential forgery under a chosen-message attack, as shown in [6].

4. Our proposed approach

In this work, we develop techniques that can be applied to prove security from static assumptions for new signature by Fuzzy Controller. Our work contains, fuzzy controller simulating by VC++ for enhancing security of dual signature (DS). Our work prevent of Desmedt and Odlyzko's attack (chosen-cipher text attack) on RSA encryptions and chosen-message attack on RSA Signatures. When hacker wants to attack on RSA encryption with chosen text attack cannot access to plain text because plaintext converted to fuzzy by fuzzy controller.

4.1 Dual Signature Operation with Fuzzy Controller

The operation for dual signature with Fuzzy Controller is as follows:

- Take the hash (SHA-1) of the payment information (PI) and order information (OI).
- These two hash values are connected [H (PI) || H (OI)] and then the conclusion convert to fuzzy data (dw fuzzy function) by fuzzy controller and then is Hashed.
- Purchaser or Customer encrypts the final hash with a private key creating the dual signature (DS).

$$\mathbf{DS = E_{KRC}\ [H(FZ(H(PI) \| H(OI)))\ ]}$$

Dual Signature (DS) Operation with Fuzzy Controller is shown in figure 2.

ISSN:2319-7900

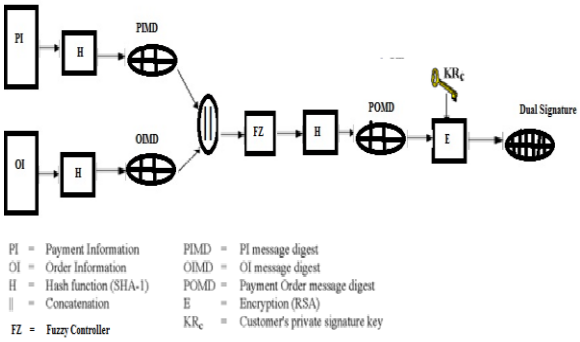

Fig 2. Dual Signature Operation with fuzzy Controller.

4.2 DS Verification by businessman or Merchant:

- The merchant has the public key of the purchaser or customer gained from the customer's certificate.
- Now, the businessman or merchant can calculate two values:

H(FZ(PIMD || H(OI)))

D_{KUC} [DS]

- Should be equal.

4.3 DS Verification by Bank

- The bank is in ownership of Dual Signature (DS), PI (payment information), the message digest (MD) for OI (OIMD), and the customer's public key, then the bank can calculate the following:

H(FZ(H(PI) || OIMD))

D_{KUC} [DS]

5. Conclusion

In this work, we develop techniques that can be applied to prove security from static assumptions for new signature by Fuzzy Controller. Our work includes, fuzzy controller simulating by VC++ and designing Input/output card cause a control power stabilizer for enhancing security of dual signature. Our work prevent of Desmedt and Odlyzko's attack (chosen-cipher text attack) on RSA encryptions and chosen-message attack on RSA Signatures. When hacker wants to attack on RSA encryption with chosen text attack cannot access to plain text because plaintext converted to fuzzy by fuzzy controller.

10. References

[1] Behrouz A. Forouzan ,Cryptography and Network Security (Sie). Edition, 2. Publisher, McGraw-Hill Education (India) Pvt Limited, (2011).

[2] Zadeh Lotfi A, "Fuzzy Logic issues contentions and perspectives",IEEE International Conference on Acoustics, Speech, and Signal Processing,2012.

[3] Y. Desmedt and A. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes, Proceedings of Crypto '85, LNCS 218, pp. 516–522,2012.

[4] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, CACM 21, 1978.

[5] J.-F. Misarsky, how (not) to design RSA signature schemes, Public-key cryptography, Springer-Verlag, Lec- tures notes in computer science 1431, pp. 14–28, 2012.