ADDING DIGITAL SIGNATURE SECURE DOCUMENT WITH PHYSICALLY UNCLONABLE FUNCTIONS

[1]A.S. Sai venkatesh, [2]M.B.Bose

[1]II Year M.E (CSE) PITS, Thanjavur, [2]Assistant Professor, CSE Dept., PITS, Thanjavur

E-mail id - saivenkatesh696@gmail.com

Abstract--**This project concentrates on information and forensics analysis under information security. Information security is the currently must needed and wide spreading technology. Algorithm in securing data on network and in personal computers is a very big issue. This project proposes a new algorithm which implementing digital signature in forensics security and data security to trace and analyze data wherever it gets transmitted. It is used to maintain the uniqueness, stability, security and tractability of the data over the network and in systems. It is also used to analyze duplication of files over the network and file transmission.**

Keywords:Digital Signature, Physically Unclonable Functions, File Tracking

1-INTRODUCTION

Digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message [1], as well as acknowledging informed consent by the signer. A visual digital signature scheme is a new and simple method to enable visual verification of an image without the need to perform heavy and complex cryptographic computations. Instead of generating, computing and manipulating large integers as in the classical digital signature schemes, this method generates shadow images known as visual shares and manipulates them by using the simple Boolean OR operation.

1.1 Using Digital Signature

Documents in digital format are increasingly becoming a common means for a wide range of information types, such as transaction records, books, scientific work, contracts, and even governmental decrees. In several cases these documents must be preserved for long periods of time, for future control and accounting purposes [2], for evidential reasons or for the protection of an entity's interests. The value of the archived documents depends on the existence of a digital signature [3], which is the principal expression of an author's intent, while it ensures the integrity of the document. The preservation of the readability, the verifiability and the validity of the digital signature are, thus, crucial for the future value of the documents.

1.2 Digital Signatures in Existence

However, the existing visual digital signature scheme has the following drawbacks. First, its security is not based on NP-hard problem. Therefore there is a possibility the method can be attacked. Second, since the existing visual digital signature scheme is using the Boolean OR operation (here OR operation means superimposing the shares) [4], the superimposing of two shares is often resulting in dark image in which there will be more bit 1's than bit 0's. Consequently, the superimposing step in this scheme has to be repeated many times in the process of avoiding from getting full black shares. As the result, the computation cost of this scheme is high. The digital signature algorithms uses some sort of complex operations aims to prevent the data from being accessible only for the authorized users, and

computing such operations could exhaust the systems with limited computational resources [5], the problem statement affects the integrity of the data directly and minimizes the security level to facilitate the process of penetration, then the algorithms must be selected depending on the degree to maintain the integrity of the information regardless of the type of device.

1.3 Key Generation in Digital Signature

The key generation procedure is used to generate the keys that are used by the signing procedure and the verifying procedure. Each time it is used the procedure generates a key pair consisting of a Private/signature key and the corresponding Public/verification key. It is important to note that the key generation procedure uses a random number generator and will generate a different pair each time it is used. SK is always known as the secret key because in applications the signing key is kept secret. PK is always known as the public key [6], the verification key is distributed to all users who want to verify signatures.The producer generates a signing process to transform/change the data from its original format to a new protected form. Each time it is used the procedure takes as input a signature key generated using the key generation procedure and data from some pre-determined data space. The signing procedure transforms the data and produces a signature as an output for the producer or the legal owner.

1.4 Transmitting Digital Signature

Consumers who receive desired data packet in reverse need to be able to check that the signature appended to the message is correct, in the sense that it is a value which would be produced if the signing procedure was applied to the received data packet using the Producer's signing key. The verifying procedure takes as input the data and signature together with the public key of the purported consumer and then either accepts or rejects the signature. If the verifying procedure outputs 'Accept,' then the message are accepted as valid; otherwise it is rejected as invalid and the consumer sends a new interest packet.

1.5 Objective of this work

The objective of this work is to present a digital signature scheme where the signature verification process is based on trust relationships, data and technologies that are available at the moment of verification. The basic idea towards this objective is the elimination of any dependency on obsolete trust relationships, data, and technologies that may have existed in the past, but are subsequently invalidated. The idea focuses on the preservation of trust in the information needed to verify the identity of the signer of a document in a ceaseless way. This is achieved by a continuous successive trust transition to new entities, data, and technologies.

2. RELATED WORK

2.1 Location Identification with Digital Signature

This model presents PriLA, a privacy-preserving location authentication framework in Wi-Fi networks. PriLA [7] extracts the inherent CFO and CSI signatures from legacy Wi-Fi preambles to verify users' locations without compromising their privacy. They have prototyped PriLA to demonstrate its feasibility and merits. PriLA is a clean-slate design that is transparent to upper layer protocols, and can be integrated into OFDM-based [8] Wi-Fi devices without hardware modifications. With those features, they believe that PriLA can be easily applied to existing LBS systems with a slight upgrade.

2.2 Digital Signature is Formalization and Accountability

They formalized the notion of accountable OFE [9], where both the signer and the third party are responsible for their behaviors. This not only is the first complete definition since its seminal introduction a decade ago but also provides a feasible approach for the design of accountable OFE with other properties. As an example, they proposed a generic (and also the first) design of OFE where the third party is transparent and

accountable. The design is based on several well-studied cryptographic primitives and satisfies all security requirements defined in this model. A concrete instance was also provided to demonstrate that the generic construction is very efficient to instantiate. the model only makes the first step towards the formalization of accountable OFE with a transparent third party, and there are some issues that need further investigation. The three kinds of accountability defined in this model only capture the basic requirements of accountable OFE, in the sense that each accountable OFE protocol must have those properties. There would be other specific requirements of accountability within concrete scenarios, and identifying those requirements is one of the future work directions. On the other hand, the protocol is only proved secure under the random oracle assumption. While random oracles have been widely used in security proofs, a provably secure protocol without random oracles is certainly more desirable.

2.3 Digital Signature with Cryptograpy

Cryptographic primitives are fundamental building blocks for security protocols. It is not too much to say that the selection and integration of appropriate cryptographic primitives into the security schemes determines the efficiency and energy conservation of the whole scheme. In this model, they showed how to integrate a set of the cryptographic primitives into a SDA scheme in [10] HSNs to achieve security requirements. They proposed a practical SDA scheme, Sen-SDA [11], based on the combination of the HE scheme, EC-ElGamal+ and the pairing-free IBS scheme, mID-Sch and the batch verification with BQS for finding invalid signatures in heterogeneous clustered WSNs. Sen-SDA provides end-to-end confidentiality and hop-by-hop authentication. They determined the size of a cluster depending the ratio of the number of invalid signatures to minimize the efficiency of CHs' batch verifications. They then presented the feasibility of the scheme in the HSNs demonstrating software implementation results on MICAz [11] and Tmote [12] Sky.

3. PROBLEM DEFINITION

3.1 Existing Approach

Existing system proposes a theoretical study and a full overview of the design, evaluation and optimization of a PUF based on transient element ring oscillators (TERO-PUF). Existing system shows how, by following some simple design rules and strategies, designers can build and optimize a TERO-PUF with state of the art PUF characteristics in a standard CMOS technology. To this end, they analyzed the uniqueness, steadiness and randomness of responses generated from 30 test chips in a CMOS 350nm process in nominal and corner voltage and temperature conditions. Response generation schemes are proposed and discussed to optimize the PUF performances and reduce its area without noticeable loss in its output quality. In particular, existing idea shows that the large area of the basic blocks in the TERO-PUF is balanced by the high level of entropy extracted in each basic block. Guidelines are provided to balance reliability and randomness of the responses and the design area.

3.2 Proposed Approach

The idea behind the proposed system is derived from the existing TERO-PUF methodology. But instead of using it as the binary data, the proposed algorithm DS-PUF : Digital Signature in Physically Unclonable Functions will considers the data as the Hexadecimal data. In physical state the data will be considered as the binary value but in logical level of application layer it is considered as the Hexadecimal Value. So the Digital Signature will be more secure and more applicable to the network and application layers. This methodology can be improved to implement in Network and data Security.

4. SYSTEM DESIGN

4.1 Input File Preprocessing

In this modules that support insertion of files into the currently processed input file. The name of the file to be inserted is computed from information of the current input file. Such computations have to be executed immediately while the input is being read by the client and it give to the server.

4.2 Binary to Hexadecimal Conversion

The client data can be taken by the server. The server is converting the binary data in to hexadecimal data.Binary data is a type of data that is represented or displayed in the binary numeral system. It is numerically represented by a combination of zeros and ones. Hexadecimal data is a positional numeral system with a base, of 16. It uses sixteen distinct symbols, most often the symbols 0–9 to represent values zero to nine, and A, B, C, D, E, F (or alternatively a, b, c, d, e, f) to represent values ten to fifteen.

4.3 Secret Key Generation

A secret key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted or decrypted. In this system that uses pairs of keys: public keys that may be disseminated widely paired with private keys which are known only to the owner. There are two functions that can be achieved using a public key to authenticate that a data originated with a holder of the paired private key or encrypting a data with a public key to ensure that only the holder of the paired private key can decrypt it.

4.4 Hexadecimal Encryption on Data

Enter the key to be used to encrypt or decrypt the data in the field below. If Text is checked, the key may consist of any sequence of up to 1024 characters; for maximum security, if the key consists of a sequence of words (many people find it easier to remember a phrase instead of a random sequence of characters), it should be at least 60 characters in length. If Hexadecimal is checked, the key is given as a sequence of hexadecimal digits: 0-9, a-f (or A-F), which should be 32 bytes (64 hexadecimal digits) in length for maximum security. The Generate button may be used to create a key in either text or hexadecimal format (depending on which button is checked) sufficiently long to provide maximum security using a high quality pseudorandom number generator seeded from the time the page was loaded, the time you pressed the Generate button, and the time of keystrokes and various other events since the page was loaded. You can generate lists of keys suitable for exchanging with correspondents using the companion Pass Phrase Generator page.

4.5 Addition of Digital Signature

In this module the server add the digital signature in to the file.A digital signature is a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means who created the document and that it has not been altered in any way since that person created it. It relies on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one client is sending to another and encoding it into a form that only the other client will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These are the two processes work for digital signatures. After added digital signature in to the file. The file can be send to the client in secured way. So another client cannot view the file without having the secret key.

4.6 Hexadecimal Decryption on Data

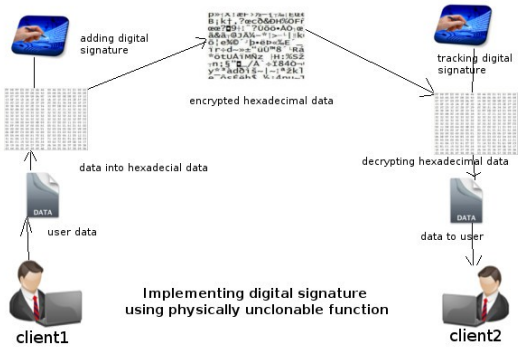
To decrypt an enciphered message, paste it in the box below, enter the key with which it was encrypted in the Key box at the top, and press the Decrypt button. The decrypted text will be placed in the Plain Text box above. Text before and after the encrypted message is ignored, and the encoding used by the message is determined automatically. You can decrypt only one message at a time; if more than one encrypted message is pasted into the box below, only the first will be decrypted.

4.7 Validation of Digital Signature using Forensics Analysis

The digital signature provides a means of integrity checking. This is done to provide assurance for the receiver that the data was in fact sent by the assumed party. The integrity plays a critical role in virtual society and it's important to protect it from coming out to the public ensure data integrity so that every important data has to be signed by its owner in order to send it safely inside the network. In this they are using Forensic Data Analysis (FDA) is a branch of Digital forensics. It examines structured data with regard to incidents of financial crime. The aim is to discover and analyse patterns of fraudulent activities. Data from application systems or from their underlying databases is referred to as structured data. Forensics analysis that support to investigations can involve a wide range of activities, from simply extracting logical files to recovering and interpreting fragments of digital data to determine the activities that occurred on the digital device. Similarly, Forensics Analysis assures that none could open the data except authorized users. The digital signatures in use today can be classified according to the high underlying mathematical problem, which provides their security to the client.

4.8 Hexadecimal to Binary conversion

Hex, or hexadecimal, is a number system of base 16. This number system is especially interesting because in the casually used decimal system they have only 10 digits to represent numbers. As hex system has 16 digits, the extra needed 6 digits are represented by the first 6 letters of English alphabet. Hence, hex digits are 0,1,2,3,4,5,6,7,8 and 9 A, B, C, D, E, F. This number system is the most commonly used in mathematics and information technologies. Binary is the simplest kind of number system that uses only two digits of 0 and 1. By using these digits computational problems can be solved by machines because in digital electronics a transistor is used in two states. Those two states can be represented by 0 and 1. Finally the hexadecimal data is converted in to binary data.



5. RESULT AND DISCUSSION

The results that were obtained for all the performance measurements have been categorized according to the dependent variables. The goal with this round of tests was to provide recommendations regarding the chosen algorithms with respect to their performance and compared to the level of security provided. They suspended RSA algorithm from upgrading its performance for the reason that installing such algorithm on light-weight devices will adversely affect their performance and delay the decryption process. Hexadecimal encryption in counterpart could be a replacement for RSA system, their compatibility to be installed in any system with different memory sizes and CPU description and parameters, Hexadecimal Encryption provide the same level of security as RSA but with shorter keys: The smaller key sizes of Hexadecimal Encryption potentially allow for less computationally able light-weight devices and wireless systems to use cryptography for secure data transmissions, data verification and offers less heat generation and less power consumption, less storage space and offers an optimized memory and bandwidth and faster signature generation. One of the objective were to equilibrate Hexadecimal encryption and RSA and improve their times. The Montgomery method they employed offers an optimized multiplication sequences which aims to speed up the regular Hexadecimal Encryption algorithm process. The method changed the state of the regular

algorithm's verification time from slow to fast and the algorithm's signing time from fast to faster.

6. CONCLUSION

RSA and Hexadecimal Encryption used to protect the data packet inside the NDN network and to recommend the preferred one depending on the results we've got. In addition, the system considered that the time is an important factor that a user wouldn't wait the whole day waiting for encrypting and decrypting the data, the work on re-sampling the operations would speed up the signatures algorithm while maintaining the same security level, proposed system presents the Montgomery method aims to accelerate the signature scheme for better performance and the reduction of the wasted time. To compare the evaluation performance of the RSA and Hexadecimal Encryption digital signatures this system used Open-SSL for comparison, and as results it is found that: The key generation time for Hexadecimal Encryption was significantly faster than RSA due to the difference in the key lengths. The RSA keys that are generated using large prime numbers thus take significantly longer than the smaller Hexadecimal Encryption keys that are generated. The execution time between RSA and Hexadecimal Encryption was significant. This result is expected since the RSA keys are significantly larger than the Hexadecimal Encryption keys. The verification time between regular Hexadecimal Encryption and RSA was significant to. This is most likely due to the fact that the regular Hexadecimal Encryption uses a complex operations rather than RSA. the algorithm(Modified Hexadecimal Encryption) has shorten the differences between Hexadecimal Encryption and RSA in terms of signing and verification time which could lead us to a new level where that can be grouped security, speed, stability and compatibility together.

REFERENCES

[1] P. S. Ravikanth. Physical One-Way Functions. Ph.D. Dissertation. Massachusetts Institute of Technology. 2001.

[2] D.E. Holcomb, W.P. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. Computers, IEEE Transactions on, 58(9): 11981210. Sep. 2009.

[3] S.S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. In Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on, pp. 6770. Jun. 2008.

[4] D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas. Extracting secret keys from integrated circuits. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 13(10): 12001205. Oct. 2005.

[5] G.E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In Design Automation Conference, 2007. DAC 07. 44th ACM/IEEE, pp. 914. Jun. 2007.

[6] H. Onodera. Variability: Modeling and its Impact on Design. IEICE Trans. Electron. Mar. 2006.

[7] S. Devadas, E. Suh, S. Paral, R. Sowell, T.Ziola, and V. Khandelwal. Design and Implementation of PUF-Based "Unclonable" RFID ICs for anti-counterfeiting and security applications. In Inter. Conf. on RFID, IEEE 2008, pp.58-64. 2008.

[8] A. Maiti, J. Casarona, L. McHale, and P. Schaumont. A large scale characterization of RO-PUF.

[9] N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov. True-randomness and pseudo-randomness in ring oscillator-based true random number generators.

[10] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robinson, and P. Maurine. Contactless electromagnetic active attack on ring

oscillator based true random number generator. In Proc. on Int. Work.