International Archive of Applied Sciences and Technology
Int. Arch. App. Sci. Technol; Vol 6 [1] March 2015: 31-36
© 2015 Society of Education, India
[ISO9001: 2008 Certified Organization]
www.soeagra.co/iaast.html

IAAST
ONLINE ISSN 2277- 1565
PRINT ISSN 0976 - 4828

CODEN: IAASCA ORIGINAL ARTICLE

New Security Concept On Information Transfer In Network Security Using Digital Signature

[1]Prerna Rai, [2]Pulkit Rai
[1,2]B.Tech,Computer Science
[1]MAIET, Jaipur,[2] GGSIPU, Delhi
[1]E-mail: prernaraijain@gmail.com
[2]E-mail: pulkitraijain@gmail.com

ABSTRACT

Our objective is to provide the tools for certifying the origin of the file where it come from by using digital signature with the new concept of security tokens. When transferring important documents it is often necessary to certify in a reliable way who is actually the sender of a given document. One approach for certifying the origin of documents and files is by using the digital signature. Whenever we need to authenticate the data, messages and any kind of information transfer in any network we require verification of this data that it is coming from authorized user so for this confirmation we can use a security mechanism that is called digital signature. The digital signature allows the recipient to check the actual origin of the information and its integrity. In present scenario we are using a varity of algorithm like SHA-1, RSA and etc for providing for security and integrity of data. Digital Signatures are messages that identify and authenticate a particular person as the source of the message and indicate such person's approval of the information contained in the message. They help users to achieve basic security building blocks such as authentication and integrity. In this paper we present the basic security concept named security tokens as it will clearly help and improved while providing the security and encryption to the electronically transmitted media. For tokens to identify the user, all tokens must have some kind of number that is unique.

Keywords: RSA, SHA-1, D.S., Security Tokens

Received 18/12/2014 **Revised 27/01/2015** **Accepted 21/02/2015**

Citation of this article

Prerna R, Pulkit R. New Security Concept On Information Transfer In Network Security Using Digital Signature. Int. Arch. App. Sci. Technol; Vol 6 [1] March 2015: 31-36. DOI.10.15515/iaast.0976-4828.6.1.3136

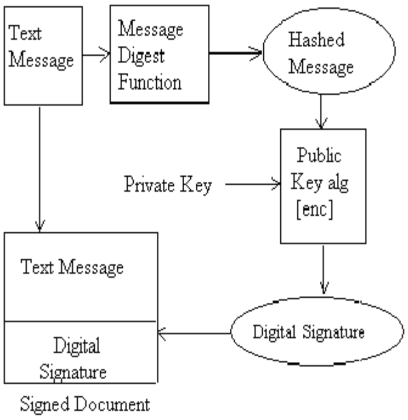
INTRODUCTION

One approach for certifying the origin of documents and files is by using the so-called technique digital signature. The idea behind digital signature is the same as the handwritten signature. A digital signature doesn't involve signing something with a pen and paper then sending to the receiver. But like a paper signature, it attaches the identity of the signer to a transaction.

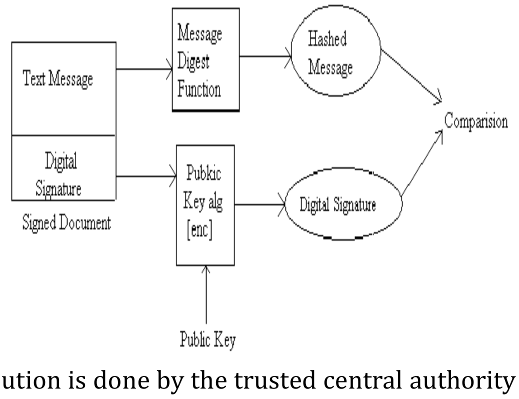
The digital signing is a mechanism for certifying the origin and the integrity of electronically transmitted information. In the process of digitally signing, additional information—called a digital signature—is added to the given document, calculated using the contents of the document and some private key. The digital signature is a number (sequence of bits), calculated mathematically when signing a given document (message). This number depends on the contents of the message, the algorithm used for signing, and the private key used to perform the signing. The digital signature allows the recipient to check the actual origin of the information and its integrity. Digital signatures can be generated by using technique public key cryptography combined with a one way hash function. This requires public-private key pair. A public key can be used to check digital signatures, created with the corresponding private key, as well as for encrypting documents that can then be decrypted only by the owner of the corresponding private key. The public keys are not secret to anybody. The private key is a number known only to its owner. With his or her private key, a person can sign documents and decrypt documents that are encrypted with the corresponding public key. To a certain extent, the private keys resemble the well-known access passwords, which are a widespread authentication method over the Internet. The public and private keys are mathematically bound cryptographic key pair (public/private key pair). To each public key corresponds exactly one private key and vice versa; to each private key corresponds exactly one public key. To use public key cryptography, one must have a public key and its corresponding private key.

WORKING

D.S. GENERATION: The following procedure is involved in the digital signature generation, if a sender wants to send receiver a text message, with digital signature, first the sender creates the text message to be signed and generates a hashed message using the message digest function. Message digest function is a mathematical function that generates a 160-bit hash code.The hash code has the property that we can generate the hash code from original message but we can not generate original message from the hash code. Once sender has the hashed message he uses the public key cryptographic algorithm and his private key to sign the hash to generate the digital signature .The signed document is sent to the receiver.[1]



D.S. VERIFICATION: Once the receiver receives the digital signature and the corresponding text message he need to calculate two values. First the hashed message of the received text is calculated using the same hashing algorithm. Then once he has the hash value he uses the decryption algorithm with sender's public key and the digital signature to retrieve the signed hash. If he can decrypt digital signature which implies that sender's private key was used to encrypt the hashed message. The final step is to compare the hash he calculated with the hash he retrieved from the encryption process. If these two hashed messages match, this implies that he retrieved the original message signed by the sender.[2]



The key generation and distribution is done by the trusted central authority called Certification Authority (CA).CA accepts the certificate applications from entities, authenticates application issues certificates to users and devices and maintains and provides status information about the certificates.

NEED FOR DIGITAL SIGNATURE

Unlike paper documents, digital documents - such as Word documents and e-mail messages have little to vouch for their authenticity and integrity. For example, e-mails do not have the identifying components that are found in a letter, such as letterhead, address of the recipient, date and traditional hand-written signature. It is also easy to forge message headers so that they appear to come from someone else.
In this environment there are circumstances when it is important for the recipient to be confident that the message has come from the person it seems to have come from and also that it has not been altered in transit. With the growing use of attachments to distribute information, it has become more important to

be able to identify the sender of an e-mail message. The risk of viruses from attachments means that people will only want to open attachments from a trusted source.

LITRATURE WORK

A Forward-Secure Digital Signature Scheme:

We have proposed a scheme in digital signature in which we keep the public key fixed but the secret signing key is not fixed and gets updated at regular intervals. The benefits of providing this scheme is that, compromise of the current secret key does not enable an adversary to the signatures belonging to the past. This can be useful to overcome the damage caused by key exposure without requiring distribution of keys. Our construction uses ideas from the Fiat-Shamir and Ong-Schnorr identification and signature schemes, which have proven to be secured based on the hardness of factoring, in the random oracle model. The construction is also quite efficient. [3]

Security enhancement for digital signature schemes with fault tolerance in RSA:

The Digital signature schemes with fault tolerance make it possible to detect errors and correct error as well during the processes of computing data and transmissions. Recently, Zhang, in 1999, and Lee and Tsai, in 2003, have respectively proposed two efficient fault-tolerant schemes based on the RSA cryptosystem. Both of them can easily check the sender's identity and also keep the identity confidential. Also, they can detect the errors and correct them. However, these schemes have a common weakness in security, that is, different messages may easily be computed that have the same signature. Thus, a valid signature could be reused in another identity. This violates the principles of digital signature. In this paper, we shall show that this security weakness existed in the two previously proposed schemes and conclude that the security imperfection may also occur in other fault-tolerant public key cryptosystems that are similar to these schemes. Furthermore, we will improve Zhang's and Lee and Tsai's schemes to overcome security weakness. [4]

Design of Hyper Elliptic Curve Digital Signature:

In computer cryptography, hyper elliptic curve cryptography system is one of the best cryptography systems. DSA signature algorithm is another advanced digital signature algorithm. In this paper, bended hyper elliptic curve cryptography system and the DSA signature standard are together analyzed. The digital signature algorithm and the digital validate algorithm are studied and improved. Here the hyper elliptic curve cryptography system is transplanted into DSA algorithm. And a digital signature based on HEC-DSA system is implemented. Quartos are used to generate the function modules, RTL circuit and simulated waveform. RTL is the circuit connection in chip. It shows the connection of the modules. Simulated waveform shows us the timing and the function of the system. The security and efficiency of the HEC-DSA digital signature system is analyzed. The digital signature designed in this paper can solve the problem of checking integrality of the file and signature ID, and most importantly it is an absolute and perfect system for the Internet operations which need identity validate. [5]

USES OF DIGITAL SIGNATURE

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances for identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures.

Below are some common reasons for applying a digital signature to communications:

Authentication

Authentication is a key concept for identifying the identity of sender. Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Non-repudiation

Non-repudiation is an important aspect of digital signatures. By this property an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

TECHNOLOGIES TO BE USED

SHA-1

The Secure Hash Algorithm was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standards(FIPS 180) in 1993 a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1.

The maximum length of a message *(in bits)* that can be hashed using the SHA-1 algorithm is one less than 2 to the 64th power. Implementation of the SHA-1 algorithm consists of six major steps and a variety of minor steps.[5]

Step1: Preprocessing

The first major step is to prepare the message for hashing. There are three minor steps included in this preprocessing step. The first minor preprocessing step is to pad the length of the message so as to guarantee that the final length is a multiple of 512 bits or 64 bytes. The second minor preprocessing step is to set the initial hash value to a standard 160-bit value. The third minor preprocessing step is to parse the padded message into blocks of 512 bits or 64 bytes each.

A. Each block is processed separately

Each block is processed separately and the hash value is updated during the processing of each block. The initialized hash value from above is the input hash value for processing the first block. The updated hash value produced by processing each block serves as the initial hash value for the processing of the next block.

B.Padding the message

All messages are padded regardless of the original length of the message. The number of bits in the pad must be such as to cause the final length to be a multiple of 512 bits. The first bit in the pad must have a value of 1. The last 64 bits in the pad must contain a binary representation of the length of the original message. All other bits in the pad must have a value of 0.

C.Processing the message blocks:

Each message block, consisting of 64 bytes, is processed in sequence. The hash value output from processing one message block forms the initial hash value for processing the next message block. The hash value output from processing the final message block is the message digest for the message.

The five remaining steps

The five remaining major steps take place and are repeated during the processing of each message block.

Step 2: Initialize the message schedule

Initialize the message schedule **W** by using the incoming 64 bytes that constitute a message block to populate the first sixteen 32-bit elements of the 80-element message schedule.

Step 3: Populate the remainder of the message schedule Populate the remaining 64 elements of the message schedule **W** by propagating the values in the first sixteen elements upward into the remaining 64 elements.

Step 4: Initialize the working variables

Set the initial values of the variables **A** through **E** to the five 32-bit segments of the incoming 160-bit hash value.

Step 5: Process the message schedule: Individually process each of the elements in the 80-element message schedule. A different process is applied to the elements in each group of 20 elements. The processing of each element results in an updated set of values for the working variables **A** through **E.**

Step 6: Update the hash value: When all 80 elements in the message schedule have been processed, use the values in the working variables **A** through **E** to update the five 32-bit segments of the hash value. This updated hash value is used as the input hash value for processing the next message block. If all message blocks have been processed, the updated hash value is the message digest for the message that has been processed.

RSA

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.[6]

Key Generation Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product *n = pq* is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1) (q-1).
3. Choose an integer e, 1 < e < phi, such that gcd (e, phi) = 1. [See note 2].
4. Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi). [See note 3].
5. The public key is (n, e) and the private key is (n, d). The values of p, q, and phi should also be kept secret.

a. n is known as the *modulus.* `
b. e is known as the *public exponent or encryption exponent*.
c. d is known as the *secret exponent or decryption exponent.*

Encryption

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer m [see note 4].
3. Computes the cipher text c = m^e mod n.
4. Sends the cipher text c to B.

Decryption:

Recipient B does the following:-

1. Uses his private key (n, d) to compute m = $c^{\wedge d}$ mod n.
2. Extracts the plaintext from the integer representative m.

PROPODSED WORK

Security Tokens: Trusted as a regular hand-written signature, the digital signature must be made with a private key known only to the person authorized to make the signature. Tokens that allow secure on-board generation and storage of private keys enable secure digital signatures, and can also be used for user authentication, as the private key also serves as verification for the user's identity.

For tokens to identify the user, all tokens must have some kind of number identity that is unique. All the approaches do not completely qualify digital signatures criteria according to some national laws. Tokens with no on-board keyboard or another user interface cannot be used in some signing scenarios, such as confirming a bank transaction based on the bank account number that the funds are to be transferred to.

Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods. Commercial solutions are provided by a variety of vendors, each with their own trade name (and often patented) implementation of variously used security features. Token designs meeting certain security standards are certified as FIPS compliant. Tokens without any kind of certification are sometimes viewed as suspect, as they often do not meet accepted government or industry security standards, have not been put through rigorous testing, and likely cannot provide the same level of cryptographic security as token solutions which have had their designs independently audited by 3rd party agencies.

There are four types of tokens:

1. Static password.
2. Synchronous dynamic password
3. Asynchronous password
4. Challenge response

This article currently focuses on synchronous dynamic password tokens.

The simplest security tokens do not need any connection to a computer. The client enters the number to a local keyboard as displayed on the token (second security factor), usually along with a PIN (first security factor), when asked to do so.

Other tokens connect to the computer using wireless techniques, such as Bluetooth. These tokens transfer a key sequence to the local client or to a nearby access point.

Alternatively, the new forms of tokens that are coming into mainstream use are mobile devices which communicate using an out-of-band channel (like voice, SMS, USSD). This makes the authentication and identity protection much stronger when compared to conventional simple synchronous dynamic password tokens.

CONCLUSION

With the advancement in technology, it is expected to get even more reliable media for communication. Our system will provide one extra concept of security token for authentication of data or messages.

One application is used for certifying the origin of documents and files is by using the digital signature. It is important for the developers to give conclusions or state the results for their work. This application will transfer the message with authentication provided by security tokens within it. It will fulfill all the needs for a reliable transfer by using efficient digital signature algorithms.

REFERENCES

1. Harn, L.; Comput. Sci. Telecomm. Program, Missouri Univ., Kansas City, MO,” New digital signature scheme based on discrete logarithm “,IEEE,1999, Institution of Engineering and Technology ,Volume: 30,p-p no. 396-398, ISSN: 0013-5194.
2. Mihir Bellare and Phillip Rogaway”, (1996). The Exact Security of Digital Signatures-How to Sign with RSA” ,1996, Volume 1070/1996, 399-416, DOI: 10.1007/3-540-68339-9_34
3. Mihir Bellare, Sara K. Miner”, (1999). A Forward Secure Digital Signature scheme”, Volume 1666/1999, 786, DOI: 10.1007/3-540-48405-1_28
4. Iuon-Chang Lin, Chin-Chen Chang (2007). Security enhancement for digital signature schemes with fault tolerance in RSA ”, India ,31st March, IEEE International Conference.
5. Kitsos, P.; Sklavos, N.; Koufopavlou, O. (2002). Electr. & Comput. Eng. Dept., Patras Univ., Greece”, “An efficient implementation of the digital signature algorithm”. p-p no. 1151 - 1154 vol.3, ISBN no.: 0-7803-7596-3.
6. Deng Jian-zhi; Cheng Xiao-hui; Gui Qiong; (2009).Dept. of Electron. & Comput. Sci., Guilin Univ. of Technol., Guilin, China “,”Design of Hyper Elliptic Curve Digital Signature”,IEEE, Information Technology and Computer Science, International Conference , 25-26 July 2009,p-p no. 45 – 47, ISBN: 978-0-7695-3688-0.