ISSN: 2321-7782 (Online)
Volume 3, Issue 11, November 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Providing Security to Confidential Information Using Digital signature

D. Shiva Rama Krishna
Assistant Professor,
Department of Computer Science and Engineering,
Marri Laxman Reddy Institute of Technology and Management.

Abstract: ***with the increasing development of information application, the security of information has become a prominent problem. It also makes the digital signature technology has been rapid developed and applied. This paper introduces the concept, characteristics, related technologies of digital signatures, and the current research state of several types of digital signature. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message and that the message was not altered in transit Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. Thus providing the services of authentication, non repudiation, data integrity.***

Keywords: Digital Signatures, Digital Signature Algorithm, Digital Signature Standard

I. INTRODUCTION

Now a day's providing security to confidential information is necessary and crucial thing. Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).to provide the security we are using public key cryptosystems. Digital signature is a public key crypto system which is used to provide Authentication, non repudiation, data integrity services to confidential information. A digital signature scheme typically consists of three algorithms;

A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. A signing algorithm that, given a message and a private key, produces a signature. A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity. Below fig shows how to create digital signature between two communication parties Bob and Alice. Where Bob creates the digital signature to the message M by using his own private key, Alice verifies the digital signature by using Bob's public key and send the acknowledgement that digital signature is valid or not

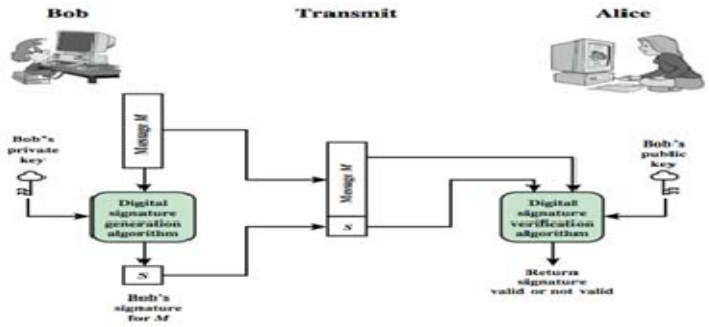

Fig 1: Digital Signature Model

II. Applications Of Digital Signature

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, 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. Fallowing are silent features or applications of digital signatures.

Authentication

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. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates 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 (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically *non-repudiation of origin*, 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.

III. Digital Signature Properties

Digital Signatures have below Properties

- Must depend on the message signed.
- Must use information unique to sender to prevent both forgery and denial.
- Must be relatively easy to produce
- Must be relatively easy to recognize & verify.
- Be computationally infeasible to forge With new message for existing digital signature with fraudulent digital signature for given message.
- Be practical to save digital signature in storage based on these properties digital signatures can be classified as two types.direct digital signature and arbirated digital signature.

There are two different types of digital signatures Direct Digital siganture, Arbirated digital signature.

Direct Digital Signature

Direct Digital Signatures involve the direct application of public-key algorithms. But are dependent on security of the sender's private-key. Have problems if lost/stolen and signatures forged. Need time-stamps and timely key revocation. digital signature made by sender signing entire message or hash with private-key can encrypt using receiver's public-key.important that sign first then encrypt message & signaturesecurity depends on sender's private-key .

Arbirated Digital Signature

Arbitrated digital signature involves use of arbiter A.validates any signed message then dated and sent to recipient requires suitable level of trust in arbiter can be implemented with either private or public-key algorithms arbiter may or may not see message.

IV. DSA ALGORITHM

The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.[1] Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 201.Below fig shows DSA Approach.

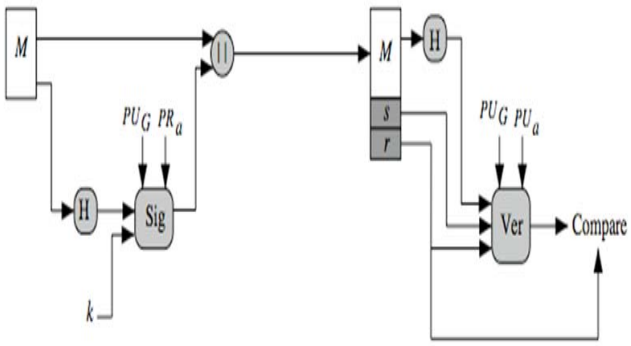

Fig 2: DSA Approch

In DSA we have key Generation, DSA signature creation, DSA Signature Verification.

Key Generation

» Have shared global public key values (p,q,g):

choose 160-bit prime number q

choose a large prime p with $2^{L-1} < p < 2^L$

where L= 512 to 1024 bits and is a

multiple of 64

such that q is a 160 bit prime divisor of

(p-1)

choose $g = h^{(p-1)/q}$

where $1<h<p-1$ and $h^{(p-1)/q} \bmod p > 1$

» Users choose private & compute public key:

choose random private key: $x<q$

compute public key: $y = g^x \bmod p$

DSA Signature creation

» To **sign** a message M the sender:

Generates a random signature key k, k<q

Nb. K must be random, be destroyed after

use,and never be reused.

» Then computes signature pair:

$R = (g^k \bmod p) \bmod q$

$S = [k^{-1}(H(M) + xr)] \bmod q$

» Sends signature (r,s) with message M

Signature Verification

» Having received M & signature (r,s)

» To **verify** a signature, recipient computes:

$W = s^{-1} \bmod q$

$U1 = [H(M)w] \bmod q$

$U2 = (rw) \bmod q$

$V = [(g^{u1} y^{u2}) \bmod p] \bmod q$

» If v=r then signature is verified

V. DIGITAL SIGNATURE STANDARD

The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the Digital Signature Standard (DSS). This Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.

In digital signature standard we are implementing digital signature algorithm. The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993.

The Digital Signature Algorithm (DSA) can be used by the recipient of a message to verify that the message has not been altered during transit as well as ascertain the originator's identity. A digital signature is an electronic version of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Below fig shows DSS approach. which provides more confidentiality and message intigrity than RSA Approach.

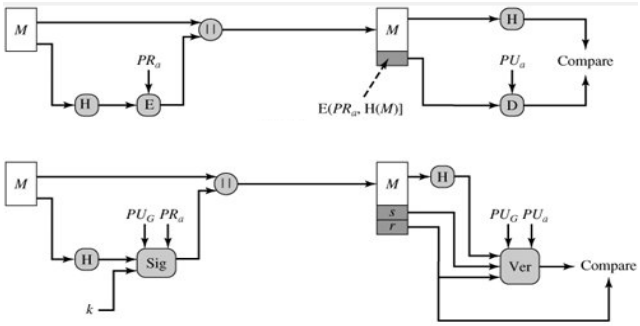

Fig3:DSS Approch

Digital Signature Generation and Verification

The DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process. For both signature generation and verification, the data (which is referred to as a message) is reduced by means of the Secure Hash Algorithm (SHA) specified in FIPS 180-1. An adversary, who does not know the private key of the signatory, cannot generate the correct signature of the signatory. In other words, signatures cannot be forged. However, by using the signatory's public key, anyone can verify a correctly signed message

VI. CONCLUSION

The digital signatures play important role in providing security to confidential information and we can make any electronic transactions by using digital signatures in secure manner. 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, as well as acknowledging informed consent by the signer. In many countries, including the United States, digital signatures have the same legal significance as the more traditional forms of signed documents. The United States Government Printing Office publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures.

References

1. V.Kavitha & K.S Easwarakumar, (2008) **"**Enhancing Privacy in Arithmetic Coding" ICGSTAIML journal, Volume 8, Issue I.
2. J.A Storer, (1988) "Data Compression: Methods and Theory" Computer Science Press. Dr. V.K. Govindan & B.S. Shajee mohan "An intelligent text data encryption and compression for high speed and secure data transmission over internet"
3. Di_e, W., and Hellman, M. New directions in cryptography. IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654.
4. Di_e, W., and Hellman, M. Exhaustive cryptanalysis of the NBS data encryption standard. Computer 10 (June 1977), 74-84.
5. D. Djenouri, L. Khelladi, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," IEEE Communication Surveys and Tutorials, vol. 7, no. 4, pp. 2–28, December 2005.
6. G. Gaubatz, J-P. Kaps, B. Sunar, "Public Key Cryptography in Sensor Networks Revisited", 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), Lecture Notes in Computer Science, vol. 3313, Springer, Heidelberg, pp. 2-18, August, 2004.
7. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: R. Lehtinen, (2006), "Computer Security Basics", 2nd Edition, O'Reilly, ISBN-10: 0-596-00669-1.
8. Shobhalokhande,Dipalisawant,NazneenSayyad,MamataYengul," E-Voting through Biometrics and Cryptography- Steganography Technique with conjunction of GSM Modem", Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012)Proceedings published in International Journal of Computer Applications® (IJCA).
9. William Stallings,"Cryptography and Network Security, Principles and Practices", Third Edition, pp. 67-68 and 317-375, Prentice Hall, 2003.
10. T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an Electronic Voting System," Security and Privacy, IEEE Symposium on, vol. 0, p. 27, 2004.
11. Crypttography and Nettwork SecuriittyFiiffttth Ediittiion by Wiilllliiam Sttallllliings Lectture slliides by Lawriie Brown
12. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.
13. B. A. Forouzan, "Cryptography and Network Security", McGraw Hill, Boston, 2008.

