Implementation of Digital Signatures

Jaipreet Kaur
Assistant Professor, Department of Electronics & Communication Engineering, GNDU Regional Campus, Sathiala (Amritsar) Punjab, India.

Sukhdeep Kaur
Assistant Professor, Department of Electronics & Communication Engineering, GNDU Regional Campus, Sathiala (Amritsar) Punjab, India.

Manjit Sandhu
Assistant Professor, Department of Electronics & Communication Engineering, GNDU Regional Campus, Sathiala (Amritsar) Punjab, India.

Abstract – With the increase in the data and data flow via internet or intranet there is a dire need of the data to be secure. The security of the data give rise to the concept of end to end encryption. There are a lot of methods that can be adopted to secure the communication between a sender and a receiver. Digital signature being one of the most important aspects of end to end encryption. The websites also need to be secured, as they are exposed to open web. Anyone with the cruel intentions can modify or even destroy the work done on the website. This paper discusses about the autonomy of digital signatures. How a sender can encrypt the message over the insecure communication channel and a receiver can decrypt the same message with the help of the provided key. Digital signatures have been accepted in several national and international standards developed and accepted by many corporations, banks, and government agencies.

Index Terms – Digital Signatures, Cryptography, Hash function, Certificate authority, Public key, Private key

1. INTRODUCTION

A digital signature is a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message. Some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is not valid. Digitally signed messages may include electronic mail, contracts, or a message sent via some other cryptographic protocol.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature but not all electronic signatures use digital signatures. A digital signature provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Digital signatures enable authentication of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

There are a number of different encryption techniques to guarantee this level of security. Digital signatures usually are transported in digital certificates e.g. encrypted electronic packages sent as e-mail attachments and increasingly used with web forms. Digital certificates are assured by trusted third parties called certificate authorities, which issue certificates and act as a guarantor of their validity. Digital certificates generally contain more comprehensive data than digital signatures, including company information, the certificate's expiration date, and so on. [4]

Digital signatures are generated by applying a mathematical formula, or algorithm, to scramble the information into a string of digits. This ensures that with the use of correct keys may unscramble them. Only the holder of the private key, the one whose signature is can sign a document with that digital signature, while anyone with the public key can verify it. Digital signatures are bound to the document to which they are applied, and cannot be copied and transferred to another document. Therefore, signatures not only help to ensure legal validity, but security as well. The digital signatures are not immune from criminal mischief but are more difficult to forge than handwritten signatures. Their use over a public-key encryption system greatly fortifies digital signatures from attack by malicious hackers.

2. USE OF DIGITAL SIGNATURE

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed document can verify both that the document originated from the person whose signature is attached and that the document has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated.

A significant benefit to the agency is in the reduction of paper handling and maintaining the data in a digital format. Signing documents digitally will enable and greatly facilitate the development of an Engineering Data Management System resulting in greater project delivery efficiency.

3. DIGITAL SIGNATURE CREATION

The use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature. Digital signature creation uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

Creating a digital signature requires software, a signing certificate, and optionally a piece of hardware to provide further security with a signer’s private key. Creating the signing certificate involves creating a public-private digital key pair and optionally obtaining the services of a Certificate Authority. The public key certificate creates proof of the identity of the signer and made available to anyone who needs to verify the signature. The combination of the public key and proof of identity result in a public key certificate also called a signer's certificate. The private key is something kept only by the signer. The document is signed with the private key. The public and private keys are related mathematically. Knowing the public key allows a signature to be verified but does not allow new signatures to be created. If the private key is not kept private, then someone could maliciously create the original signer’s signature on a document without consent.

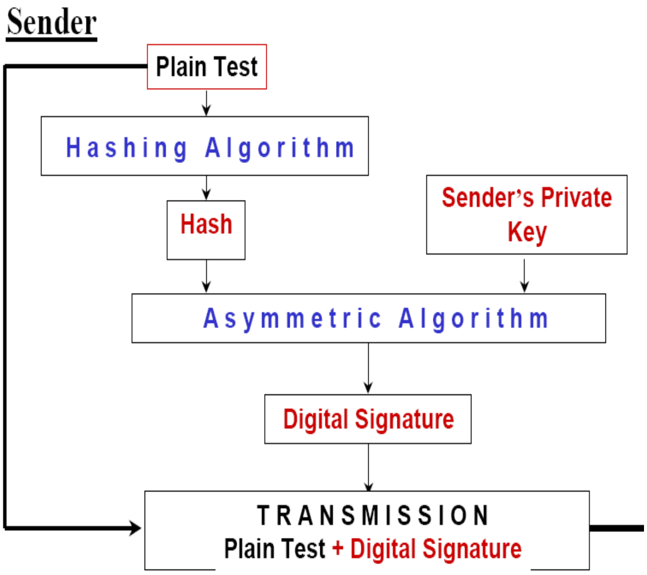

Figure 1 Digital Signature Generation [2]

4. DIGITAL SIGNATURE VERIFICATION

Digital signature verification is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

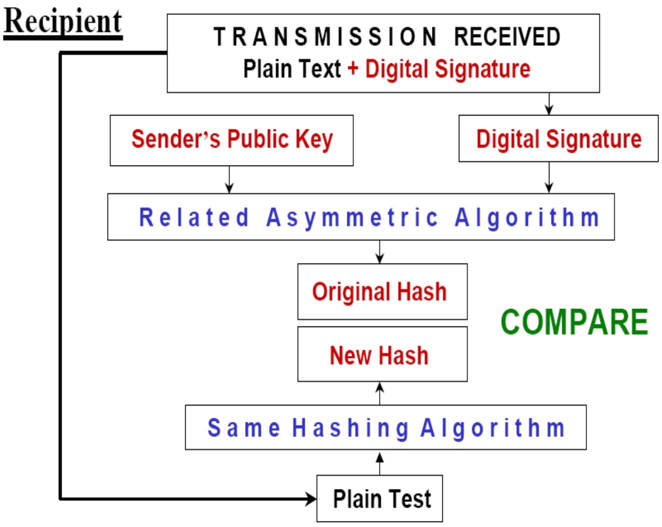

Figure 2 Digital Signature Verification [2]

To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. The solution to this is to use a trusted third party to associate an identified signer with a specific public key. That trusted third party is referred to as a Certification Authority.

A self-signed certificate is one that is created by the individual signer without the services of a certification authority and should be avoided. Digital IDs provided by 3rd parties are generally considered more secure, because an independent certificate authority has ratified them. A signature applied using a self-signed certificate signature tells a document recipient that "This document is valid, and I am authorized to sign it," while a signature applied using a 3rd party digital ID tells them that "This document valid, I am authorized to sign it, and certificate authority verifies my identity." This additional assurance can make a big difference when it comes to legal documents or those sent out to a wide audience.

To associate a key pair with a prospective signer, a Certification Authority issues a certificate, an electronic record which lists a public key as the "subject" of the certificate, and confirms that the prospective signer identified in the certificate holds the corresponding private key. The Certification Authority performs a background check on each individual that is assigned a signing certificate. [5]

New ways of verification are being developed daily. Biometrics and other methods keep getting formulated and incorporated into the information technology industry. One interesting biometric authentication mechanism developed by a leading Japanese biometric company has found a way to get your DNA into a pen. You sign a document and it is digitally scanned. This document then can be scanned in the future to verify its authenticity. Identity should be verified whenever there is doubt of the 3rd party being whom they say they are or when there is personal information at risk. Personal information like credit card details and banking information should be kept safe using digital certification as one of the security layers. Some banking institutions require that a user verifies his/her identity by validating identification credentials using a digital certificate. Important e-mail can also use Digital signatures that verify that the e-mail is from the originating sender and that it has not been tampered with. On many occasions users are unsure if they are dealing with reputable suppliers of institutions. Digital certification gives the user a sense of legitimacy and formalizes the process. It ensures that the company that the user is dealing with has a registration with a trusted authority and that the transaction is guaranteed to be done with the intended parties.

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 which, given a message and a private key, produces a signature.
- A signature verifying algorithm which given a message, public key and a signature, either accepts or rejects.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

5. COMPONENTS OF DIGITAL SIGNATURE

These are the following components used in digital signature:-

1. **Your public key: -** This is the part that any one can get a copy of and is part of the verification system.
2. **Your name and e-mail address: -** This is necessary for contact information purposes and to enable the viewer to identify the details.
3. **Expiration date of the public key: -** This part of the signature is used to set a shelf life and to ensure that in the event of prolonged abuse of a signature eventually the signature is reset.
4. **Name of the company: -** This section identifies the company that the signature belongs too.
5. **Serial number of the Digital ID: -** This part is a unique number that is bundled to the signature for tracking ad extra identification reasons.
6. **Digital signature of the CA (certification Authority): -** This is a signature that is issued by the authority that issues the certificates.
7. **Message hash algorithm: -** perform a mathematical calculation on the document and generate a hash value unique to the message8.
8. **Encryption algorithm: -** accept the private key and a hash value to generate a digital signature or accept public key and a digital signature to generate a hash value.

6. DIGITAL SIGNATURE WORKING

To create the digitally signed document, pass it through a message hash algorithm. The algorithm generates a hash of the document that is a checksum of the contents of the document. The message hash can be encrypted with private key. The result is a digital signature. The digital signature is appended to the document to form a digitally signed document. When receiver receives the document, it passes the document contents through the same message hash algorithm and creates a new hash. At the same time, sender uses public key to decrypt digital signature, thereby converting the signature to the original hash. Sender then compares the newly generate hash and the original hash. If the hashes match, recipient can be sure that the document received is really from sender and no one is altered it during transmission. If the hashes don't match, recipient knows that tampering or a transmission error changed the document.

7. BENEFITS OF DIGITAL SIGNATURES

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

- 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 sender and receiver of a message want the confidence that the message has not been altered during transmission. The encryption hides the contents of a message but there is possibility to change an encrypted message without understanding it. Digital certificates also verify date and time so that senders or recipients can not dispute if the message was actually sent or received.

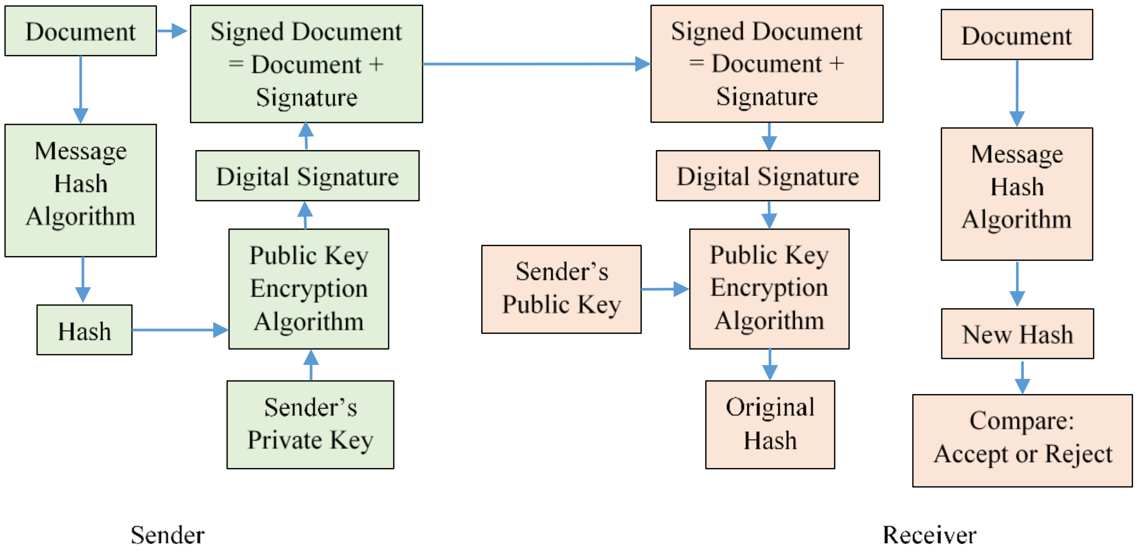

Figure 3 Transmission and reception of digital signature

8. DRAWBACKS OF DIGITAL SIGNATURES

No security system is perfect. Here is a list of the major weaknesses of this one. Despite their usefulness, digital signatures alone do not solve the following problems:

- Digital signature algorithms and protocols do not inherently provide certainty about the date and time at which the underlying document was signed. The signer might have included a time stamp with the signature, or the document itself might have a date mentioned on it. Regardless of the document's contents, a reader cannot be certain the signer did not, for example, backdate the date or time of the signature. Such misuse can be made impracticable by using trusted time stamping in addition to digital signatures.
- In a cryptographic context, the word repudiation refers to any act of disclaiming responsibility for a message. A message's recipient may insist the sender attach a signature in order to make later repudiation more difficult, since the recipient can show the signed message to a third party (e.g., a court) to reinforce a claim as to its signatories and integrity. However, loss of control over a user's private key will mean that all digital signatures using that key, and so ostensibly 'from' that user, are suspect. Nonetheless, a user cannot repudiate a signed message without repudiating their signature key. This is aggravated by the fact there is no trusted time stamp, so new documents (after the key compromise) cannot be separated from old ones, further complicating signature key invalidation. A non-repudiation service requires the existence of a public key infrastructure (PKI) which is complex to establish and operate. The Certificate authorities in a PKI usually maintain a public repository of public keys so the associated private key is certified and signatures cannot be repudiated. Expired certificates are normally removed from the repository.
- Someone could steal your private key from your computer. Protecting your private key with a password is highly recommended, so that a stolen private key is worthless (and don't store the password on the same computer!).
- Digital signatures carry a lot more authority than a simple return address, because the forgery is so much more difficult. If you lose your certificate and password, you have a problem because mail with a digital signature is more authoritative. The best thing to do in that case would be to completely stop using the email address associated with the stolen certificate, and start again.
- Some email clients are not compatible with the standard, such as older browsers and many of the web-mail sites. To the users of those the signature appears as an attachment full of weird text, and they get no validation of the signature. MIME is the standard for sending attachments, and SMIME means Secure MIME. It would be hard to send signed mail from a web-mail site.

9. CONCLUSION

The digital signature provides the legal elements of a traditional handwritten signature and enhanced security, integrity, and authenticity. The digital signatures minimize the risk of dealing with imposters and the risk of undetected message tampering and forgery and retains a high degree of information security. The one-way hash function, asymmetric encryption and sophisticated chip card system cause secure proceedings. Today digital signatures are under way and can only be seen as an amendment to traditional procedures. Currently, the PKI-digital signature is the best type of signature for electronic contracts. PKI-digital signature software is inexpensive and the technology is mathematically improbable to break. With future advances in technology, other types of electronic signatures may replace the PKI-digital signature. Regardless of the technology used, digital and electronic signatures are an increasingly significant part of commerce and will continue to evolve.

REFERENCES

[1] Branchaud, Marc, “A Survey of Public-key Infrastructures”, Department of Computer Science, McGill University, Montreal, 1997.

[2] Curry, Ian, Entrust Technologies, “Key Update and the Complete story on the Need for Two Key Pairs”, version 1.2, August 2000.

[3] Goldreich, Oded, “Foundations of cryptography II: Basic Applications”, Cambridge, Cambridge Univ. Press, 2004.

[4] K. LEBERHERR, “Uniform complexity and digital signatures”, Theoret. Computer. Sci., 16, 1981, pp. 99-110.

[5] A. Menezes, P. van Oorschot, and S. Vanstone, “Handbook of Applied Cryptography”. Boca Raton, FL: CRC, 1996, T-37.

[6] Nat. Inst. Std. Technol., “Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg”, MD, 2009, Digital Signature Standard (DSS).

[7] Jianglang Feng; Jindong Li, "A New Certificate-Based Digital Signature Scheme”, Fourth International Conference on Emerging Intelligent Data and Web Technologies, pp.547,549, Sept. 2013.