Persistent Security for Electronic Documents

Basim Jamil Ali
Alyaa Hashem Mohammed
Al-Mustansiriyah University

Abstract :

Organization must take significant investment to protect the electronic documents that contain mission-critical, personal, and sensitive information.
Many information security solutions attempt to protect electronic documents only on their storage location or during transmission. The purpose of this paper is intended to provide the reader with a brief overview of relevant document security issues and technologies as well as to introduce a proposed method for persistent security for electronic document throughout its lifecycle.

Several security requirements such as confidentially, authorization, accountability, integrity, authenticity, and non-repudiation must be met to provide more effective protection for electronic document throughout its lifecycle. These requirements can be achieved by using the followings:

a) Document Control process: which can be achieved confidentially, authorization, and accountability by using encryption technique.
b) Digital signature technique: which can be achieved integrity, authenticity, and non-repudiation by using secure hash algorithm-1(SHA-1) and encryption technique.

1. Introduction

As organizations move more business processes online, Protecting the confidentiality and privacy of information used during some processes, as well as providing authenticity and integrity are essential in business processes online. Because many automated processes rely on electronic documents that contain mission- critical, personal, and sensitive information, organizations must make significant investments to protect these documents. There are three main reasons that organizations need to address the security of electronically shared documents:

- Regulatory requirement: Many companies are directly or indirectly affected by government mandates and regulations for providing consumer.
- Return on investment (ROI): Organizations can achieve significant ROI by using electronic business processes. Because of automated workflows allow prospects, customers, partners, and suppliers to participate, enabling organizations to reap significant cost savings while improving customer satisfaction and loyalty. However, many workflows cannot be automated

until adequate protections are put in place on the electronically shared information.

- Information security: Thefts of proprietary information are increasing, which can warn revenue, completive advantage, and customer relationships; generate negative publicity; and result in significant penalties and fines for failure to comply with privacy laws [1].

A signature is a stylized script associated with a person. It is comparable to a seal. In commerce and the law, a signature on a document is an indication that the person adopts the intentions recorded in the document. An electronic signature is any legally recognized electronic means that indicates that a person adopts the contents of an electronic message [5].

A signature is generally understood as evidence that the signatory approves of a document's contents. the signature must be able to objectively show that the signatory, by signing or printing their name, approved of a document's contents and intended to be bound by them. It is irrelevant whether the contents have been read (unless there has been some misrepresentation) [6].

2. Securing of the electronic document

The security of electronic documents signed electronically takes on the new dimension of the time to prove authenticity and remain accessible to the parties interested [1].

In creating the signed paper document, the signer verifies the contents to match their intent at signing. Upon acceptance of the contents, they formalize their intent by attaching their signature to the document. After the document is signed, the document is inspected for alterations and the signature is often compared to the signer's verifiable signature to assure the authenticity of the formalized document. Both of electronic document and the electronic signature need to be secured for similar tests of authenticity [1].

The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a base line from which to acquire, configure and audit computer systems for compliance with the policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless [3].

All of the Authenticated e-Signature solutions incorporate easy application of trusted third-party authentication. Authenticate is an authorized provider of trusted third-party authorities [2].

The objective of electronic signed documents is that as information (documents) enters the system, each information object (document) must retain its own authenticity and integrity during its lifecycle. This requires systems to not only maintain the authoritative record, but also be able to prove the integrity of the supporting document about it. The objective now includes proving the

authenticity of the documents that represent the incremental information updates to the system over the record life cycle [8].

2.1 Digital Signatures

The most full-featured and, arguably, the most secure type of e-signature is the digital signature, which relies on public key cryptography. The public key infrastructure (PKI), based on encryption technology, was created to secure transactions on the Internet. The foundation of PKI, public key cryptography, is an encryption method that uses a two-part key that consists of a public and private component. The sender is encrypted the data with the public key and the recipient is then decrypted with his/her own private key. This technology is quickly becoming the best way to ensure safe business-to-business communication using public key signing models to seal data, protect conversations, and secure the electronic audit trail [9].

Digital certificates, (electronic credentials) are a legally binding electronic confirmation for business transactions. The Certificate contains data (meta-data) about the quality and the ownership of the key pair used in the encryption (signature) process. It provides strong proof (depending on the quality and cost of the certificate issuance process) that the document sealed by the signature process has not been changed since it was signed [9].

2.2 Electronic Signatures

Signatures in the broad electronic signature category do not rely on cryptographic methods. Instead, these are often image based or biometrics-based solutions in which the characteristics of a fingerprint, the iris of the eye, or the pressure of pen on a surface is encoded digitally and then stored and transmitted by computer to verify identity. While such signatures may be "digitized"—translated from physical characteristics or actions to computer readable code—they are not "digital." Often, these methods are combined with other technologies.

Imaging technology permits an image such as a pen-and ink signature or document to be scanned and the results stored. The resulting signatures are verified when the stored digitized image is compared for verification. It is often combined with other technologies. Applications of image based electronic signatures are common; everyone has signed with an electronic pen, thus encumbering a credit card transaction at one time or another.

While these technologies are useful in authenticating individuals, they do nothing to assure long-term viability of electronic data. There is no encryption, no sealing of the transaction data. The image of the signature gathered at the check out counter can be associated with any data set without setting off any electronic "alarms". The ability to scan a retina and authenticate an individual does nothing to prevent use of that individual's identity data for fraudulent purposes. Unlike public key based digital signatures, there is nothing in this technology that is of use to the records management problem set [9].

3. Document authenticity

Document authenticity technologies help establish that a document has not been altered or tampered with, maliciously or otherwise. Authenticity technologies also provide a means of establishing who created or signed a document [1].

Both of these requirements are critical to document authenticity and to electronic records, and it's difficult to have one without the other if you can't firmly establish who created or signed a document, how can you trust that the contents have not been altered this accountability is established with physical signatures and notary seals. The reverse is also true: if you can't show definitively that a document has not been altered, how do you know that it's from a trusted source? In the paper world, this authenticity is accomplished by well-documented record-keeping practices and the formal recording and retention of original documents. When it comes to electronic documents, accountability and authenticity can be achieved through the use of digital signatures [1].

4. The Document Secure Electronic Record

Creating document secure electronic records are achieved by attaching or associating an electronic signature to create a document signifying intent [8].
Document secure electronic records are typified by documents created with digital signatures (an application of key encrypted messaging, or public key technology). The document is processed into a hash. The hash is encrypted with the signer's private key using a standard algorithm; the resulting encrypted hash, the digital signature, is attached to the document. When the document is inspected after the signing, the encrypted hash is decrypted with the public key and compared to a re-hash of the document. If the two results are the same, then the document has remained unchanged. The document has maintained authenticity [8].

5. Cryptographic signatures

The goal of cryptography is to design, implement, deploy, and make use of cryptographic systems that are secure in some meaningful way. In order to make precise statements about the security of a cryptographic system. One must formally define the characteristics of a good security policy are:

- It must be implement able through system a administrator procedures, publishing of acceptable use guidelines, or other appropriate methods.
- It must be enforceable with security tools where appropriate, and with sanctions where actual prevention is not technically feasible.
- It must clearly define the areas of responsibility for the users, administrators and management.

An electronic signature may incorporate a digital signature if it uses cryptographic methods to assure, at the least, both message integrity and authenticity. For the cryptographic mechanisms are impracticable without computers [11, 12].

In addition, no message integrity protocols include error correction, All current cryptographic digital signature schemes require that the recipient have a way to obtain the sender's public key with assurances of some kind that the public key and sender identity properly belong together, and that message integrity measures (also digital signatures) which assure that neither the attestation nor the value of the public key can be surreptitiously changed. A secure channel is not typically required. A digitally signed text may also be encrypted for protection during transmission, but this is not required when most digital signature protocols have been properly carried out. Confidentiality requirements will be the guiding consideration [6].

Cryptographic techniques can be used to provide encryption for confidentiality and electronic signatures can provide authentication and integrity of communications [7].

6. Persistent electronic document security:

More effective solution for protecting an electronic document throughout its lifecycle is to assign security requirements that are an integral part of the document itself. The following requirements define the persistent document security:

- Confidentiality: document can be accessible only by authorized person.
- Authorization: specifies what a user can do with a document.
- Accountability: keep track each recipient's use of document for each permission assigned.
- Integrity: capability for knowing that if the document has been altered.
- Authenticity: the process that can be provided the recipient to know the source of the document.
- Non-repudiation: the service that prevents the signore of the document from denying that the signed the document [10, 13].

7. The proposed method for security of electronic document:

The requirements that can be defined the persistent document security can be achieved by using document control and digital signature techniques Figure (1).

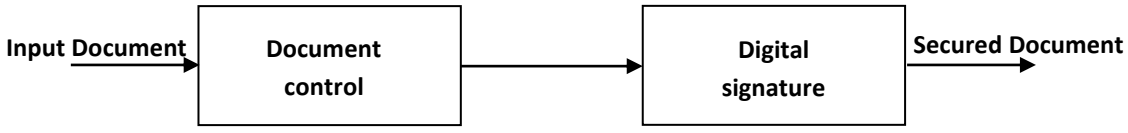

Figure (1) Document Control and Digital signature

7.1 Document control: which can be achieved Confidentiality, Authorization, and Accountability.

7.1.1 Confidentiality:

The two popular ways to achieve the confidentiality of documents are encryption and decryption. Encryption is the process of transforming information (plaintext) into an incomprehensible for (ciphertext). Decryption is the reverse process that transforms ciphertext back to the original plaintext.

There are two main types of encryption keys which are:

a- *Symmetric keys*: this cryptography technique uses the same key for both encryption and decryption.

b- *Asymmetric keys (public key)*: uses key pairs for encryption and decryption. If the first is used to encrypt the content then the second key is used to decrypt the content.

In this paper the first step is encrypted the document by using the asymmetric key and symmetric key together as a hybrid encryption. Such that the asymmetric keys (by using asymmetric algorithm-RSA) are used to protect the symmetric key, and then used the symmetric keys (by using symmetric algorithm DES) for encryption the information [14].

7.1.2 Authorization

This process can achieve the authentication by using a permission, which governs a user action while working with a protected document. Permissions can specify whether or not a recipient who has access to work with the document. For simplicity, the suggestion method is using a digital certificate which is an attachment to an electronic document, and can be issued by a Certificate Authority [7].

7.1.3 Accountability

This block can achieve the accountability by keep track each recipient's use of document for each permission assigned. Such that, user service sends an electronic document that requires an action from the recipient. Once the recipient receives the document, the user service will be notified when the recipient opens (or fail to open) the document [7].

7.2Digital signatures: Digital signatures let the recipient of information verify the authenticity of the information's origin, and also verify that the information was not altered during its lifecycle(integrity).A digital signature also provides non-repudiation ,which means that it prevents the sender from claiming that he/ she did not actually send the information[14].

7.2.1 Integrity

For simplicity one way hash function used to verify the integrity of electronic document. This function maps a message of any length into a fixed length hash value or message digest, then the recipient can determine if the message was altered or not with a hash attached to the original message. The hash can be recomputed and comparing this result with the attached hash. Hash

algorithm can be described in two stages: preprocessing and hash computation Figure (2) [10].

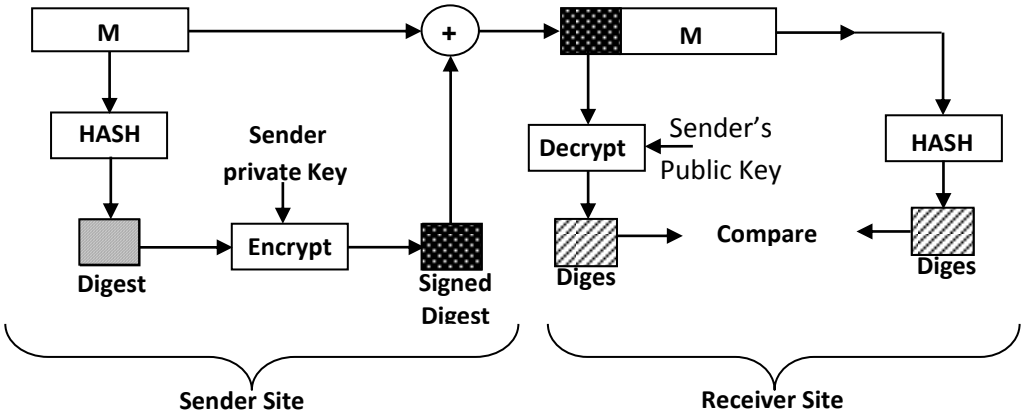

Figure (2): Secure Hash Algorithm-1

- *Preprocessing* involves padding a message, parsing the padded message into m-bit

  blocks, and setting initialization values to be used in the hash computation.
- *The hash computation* generates a message schedule from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest[10].

The suggestion method is the secure hash algorithm 1 (SHA-1) may be used to hash a message, M, having a length of n bits, where $0 \leq n < 2^{64}$. The algorithm uses:

1) a message schedule of eighty 32-bit words,
2) five working variables of 32 bits each, and
3) a hash value of five 32-bit words. The final result of SHA-1 is a 160-bit message digest.

7.2.2 Authenticity

Digital signature provides document authenticity by verifying a signer's digital identity. In this paper the suggestion method is encrypting the hash of the message with private key assuming that this is the case, the sender (A) can send a signed plaintext message (P), to the recipient (B) by transmitting [4,11,12]:

$E_B(D_A(P))$ ----------(1)

Where: D_A is the sender's (private) decryption key.

E_B is the recipient's public key.

The recipient transform it using his/her private key, as usual, yielding $D_A(P)$, as shown below:

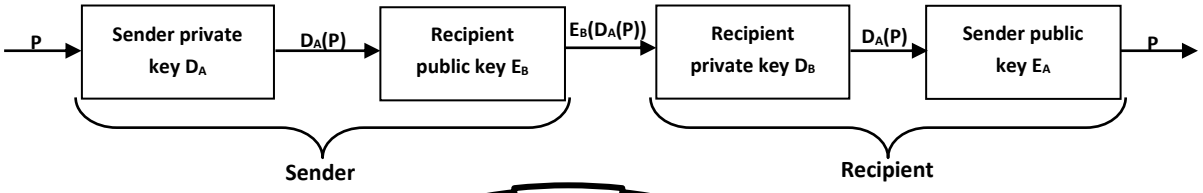

Figure (3): public key cryptography.

And the recipient has the public key of the sender, so the public key can correctly decrypt the hash of the message and use it to see if it matches a new hash of the document [11].

7.2.3 Non-repudiation

Non-repudiation is a concept, or a way, to ensure that the sender or receiver of a message cannot deny either sending or receiving such a message in future. One of the important audit checks for non-repudiation is a time stamp. The time stamp is an audit trail that provides information of the time the message is sent by the sender and the time the message is received by the receiver.

8. Conclusion

1. A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself.
2. By applying security parameters to the individual document, organization gain greater assurance in the confidentiality, authenticity, and integrity of electronically shared documents in addition to securing the communication line or storage location.
3. It can be argued that a properly secured system maintains its own integrity. Because that system retains integrity, the documents can be assumed to retain integrity from the point they enter the system. Thus, integrity of the document relies upon the security of the system. This is a valid argument and should be considered when designing security systems.
4. The proposed method provides persistent, end to end protection throughout an electronic document's lifecycle.
5. To protect sensitive electronic documents, the document control and digital signature services must be met.
6. Electronic signatures may mean using a graphic image of a signature which can't be validated, it can really be used for checking the legitimacy of document being sent.
7. Just like hand written signatures (wet signatures), its permanently attached to a document.
8. public key Infrastructure(PKI)-based electronic signatures, offer strong technology to protect against forgery by providing data integrity, author authenticity, and non- repudiation.
9. Public key cryptography plays a crucial role for protecting electronic documents.

9. References

1. www.adobe.com/..pdfs/ PDF_electronic_ records_ wp.pdf.
2. http://www.authenidate.com/index.php/Content/view/3971671.
3. N. Cowichan Duncan , "Computer, Internet and Network Systems Security", Canada Ave., Duncan, Bc, 2007
4. Oppliger Rolf, "Contemporary Cryptography", Boston, London, ARTECH House, Inc., Canton street, 2005
5. http://en.wikpedia.org/wiki/Electronic-signature.
6. www.actorsequity.org/docs/Producer/ Electronic_Contract
7. www.berr.gov.uk/ Files/ File49952.pdf.
8. http:/www.nccusl.org.
9. http://www.infosec.cu.uk/ExhibitorLibrary/98Protecting- electronic-document swp-20.pdf.
10. Behrous A. Forouzan, "Data Communication and Networking", 2006.
11. Anderw S.Tanenbaum, "Computer Ntworks",1996.
12. Dorothy Elizabeth, "Cryptography and Data Security",1982.
13. William Stallings, "Data and Computer Communication",2004.
14. http:/ / www.nai.com/An introduction to cryptography.

الخلاصة:

يجب ان تأخذ المؤسسات اهتمامها البالغ لحماية الوثائق الالكترونية والتي تحتوي على المعلومات الحساسة والشخصية والمعلومات المهمة. العديد من الحلول لامن المعلومات تحاول حماية الوثائق الالكترونية عند مواقع خزنها هو عند ارسالها.الغرض من هذ البحث هو تزويد القارىء بنبذة عامة ومختصرة بكل ما يتعلق بامنية الوثائق الالكترونية وتقنياتها، اضافة الى تقديم طريقة مقترحة لاستمرارية أمنية الوثيقة الالكترونية خلال دورة حياتها.

هنالك عدة متطلبات امنية يجب ان تلبى لتجهيز حماية فعالة للوثيقة الاكترونية خلال دورة حياتها مثل (السرية،والتفويض،والمسؤلية،وتكاملية أو سلامة،والاصالة،وعدم النبذ او الانكار). ويمكن تحقيق هذه المتطلبات باستخدام مايلي:

أ. عملية سيطرة الوثيقة: والتي تحقق متطلبات السرية،والتفويض،والمسؤلية باستخدام تقنية التشفير.

ب. تقنية التوقيع الرقمي: والتي تحقق متطلبات التكاملية (أو السلامة)،والاصالة،وعدم النبذ (او الانكار) باستخدام وتقنية الشفير. (SHA-1) خوارزمية الفرم الامنة-1