Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.111 – 117

RESEARCH ARTICLE

A Study of Electronic Document Security

Mr. Parag S.Deshmukh[1], Mr. Pratik Pande[2]

[1]*Department of Computer Science & Engineering, IBSS College of Engineering, Amravati*

[2]*Department of Computer Science & Engineering, Prof. Ram Meghe College of Engineering, Amravati*

[1] dreamsparag@gmail.com, [2] pratik.pande01@gmail.com

Abstract—This paper is an overview of relevant document security issues and technologies, as well as to introduce the suite of document security solutions. This paper also summarizes implementations for document control and digital signatures to protect electronic documents. As organizations move more business processes online, protecting the confidentiality and privacy of information used during these processes, as well as providing authenticity and integrity, are essential. Because many automated processes rely on electronic documents that contain sensitive information, organizations must properly protect these documents. Many information security solutions attempt to protect electronic documents only at their storage location or during transmission. However, these solutions do not provide protection for the entire lifecycle of an electronic document. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients. A significantly more effective solution is to protect a document by assigning security parameters that travel with it. Six criteria must be met in order to provide more effective protection for an electronic document throughout its lifecycle: Confidentiality, Authorization, Accountability, Integrity, Authenticity, and Non-repudiation. The two major security techniques used to establish these six document security criteria are document control and digital signatures. The Electronic suite of security solutions delivers document control and digital signature services that simplify the process of protecting sensitive electronic documents and forms. Organizations can easily integrate Electronic document security solutions into current business processes and enterprise infrastructure to support a wide range of simple and complex processes. The solutions dynamically protect electronic documents inside and outside the network, online and offline to provide persistent, end-to-end protection throughout an electronic document's lifecycle.

Keywords— Confidentiality; Authorization; Accountability; Integrity; Authenticity; Non-repudiation

I. INTRODUCTION

As organizations move more business processes online, protecting the confidentiality and privacy of the information used during these processes is essential. Because many automated processes rely on electronic documents that contain mission-

© 2014, IJCSMC All Rights Reserved

critical, personal, and sensitive information, organizations must make significant investments to properly protect these documents [4]. There are three main reasons that organizations need to address the security of electronically shared documents:

A. *Regulatory requirements*

Many companies are directly or indirectly affected by government mandates and regulations for providing consumer privacy. These include:

- Health Insurance Portability and Accountability Act (HIPAA)—Protection for health-related data.
- Gramm-Leach-Bliley Act—Financial privacy.
- European Union Directive on Privacy and Electronic Communications.
- Privacy Acts of Japan and Australia.
- California SB 1368—Privacy notification.
- California AB 1950—Protection of customer data [3].

B. *Return on investment (ROI)*

Organizations can achieve significant ROI by migrating to electronic business processes. 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. For instance, how can you be sure that the bank statement you received is truly from your bank (authenticity), that it has not been altered in transit (integrity), and that it has not been viewed by someone other than the intended recipient (confidentiality)?

C. *Information security*

Thefts of proprietary information are increasing, which can jeopardize revenue, competitive advantage, and customer relationships; generate negative publicity; and result in significant penalties and fines for failure to comply with privacy laws. Many information security solutions attempt to protect electronic documents only at their storage location or during transmission. For example, organizations rely on document management systems and virtual private networks (VPNs) to protect documents. With this approach document security remains a problem because these solutions secure only the communication line or storage site; they do not provide protection for the actual content of an electronic document throughout its lifecycle. When the document reaches the recipient, the protection is lost, and the document can be intentionally or unintentionally forwarded to and viewed by unauthorized recipients. Consequently, many organizations are forced to engage in an inconsistent combination of online and paper processes in which sensitive documents must still be printed and physically delivered to achieve adequate security. As a result, the potential benefits of online processing cannot be fully realized.

II. HOW TO PROVIDE PERSISTENT DOCUMENT SECURITY

A significantly more effective solution for protecting an electronic document is to assign security parameters that are an integral part of the document itself. The following criteria define persistent document security [2]:

- Confidentiality—Who should have access to the document?
- Authorization—What permissions does the user have for working with the document?
- Accountability—What has the recipient done with the document?
- Integrity—How do you know if the document has been altered?
- Authenticity—How do you know where the document came from?
- Non-repudiation—Can the signatory deny signing the document?

© 2014, IJCSMC All Rights Reserved

Fig 1: Six key criteria for providing persistent document security

The following sections survey the major technologies used to provide document control and digital signatures and identify the technologies Electronic has implemented for its document security solutions

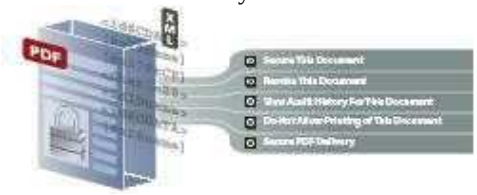

Fig 2: Document control options

III. DOCUMENT CONTROL

A. Confidentiality—encryption

Encryption is the process of transforming information *(plaintext)* into an incomprehensible form *(ciphertext)*. Encryption is an effective technique for managing document access. Decryption is the reverse process that transforms ciphertext back to the original plaintext. Cryptography refers to the two processes of encryption and decryption and its implementation is referred to as a *cryptosystem*. Popular encryption systems use the concept of keys. An encryption key is data that combines with an encryption algorithm to create ciphertext from plaintext and recover plaintext from ciphertext. Today, security experts widely agree on "Kerckhoff's" principle as the basis of an effective cryptosystem. Kerckhoff's principle states that the key is the only portion of a cryptosystem that must remain secret for the entire system to be secure. If the strength of the cryptosystem relies on the fact that an attacker does not know how the algorithm works, then it is just a matter of time before it can be reverse engineered and broken. Two main types of encryption keys include symmetric and asymmetric.

1) *Symmetric keys:* Symmetric key cryptography uses the same key for both encryption and decryption and is very fast and difficult to break with large keys. However, because both parties need the same key for effective communication to occur, key distribution becomes an issue. Today, common symmetric key encryption algorithms are AES, DES, 3DES, and RC4. Electronic products leverage AES (128- and 256-bit) and RC4 (128-bit), as they have evolved into very strong standards.

2) *Asymmetric keys:* Asymmetric key cryptography, also called *public key cryptography*, uses key pairs for encryption and decryption. For instance, if the first key encrypts the content, then the second key of the pair decrypts the content. Similarly, if the second key is used to encrypt the information, then the first key must be used to decrypt the content. Typically, one key in the pair is labeled as the public key and the other as the private key. An individual keeps the private key secret, while the public key is freely distributed to others who wish to communicate with the individual. When someone wishes to send the individual a confidential message, he or she can encrypt it with the freely available public key and send the ciphertext to the individual. Because the individual is the only one who has the private key, he or she is the only one who can decrypt the content.

© 2014, IJCSMC All Rights Reserved

Asymmetric keys help solve the key distribution problem, but the algorithms tend to be slower for equivalent strengths. Some common asymmetric algorithms are RSA, DSA, and El Gamal.

3) Hybrid Encryption: Security systems tend to use a hybrid solution to increase the security and speed of encrypting documents. One approach is to use asymmetric keys to protect the symmetric keys, and then use the symmetric keys for encrypting the information. This technique helps to solve both the key distribution challenge of symmetric key cryptography while solving the performance problem of asymmetric key cryptography. Electronic Acrobat software leverages hybrid approaches so single documents can be protected for multiple recipients, each possessing unique key pairs. The file size is not significantly increased during this method because the entire document does not need to be encrypted for each person. Instead, the document is encrypted with a single symmetric key and that symmetric key is encrypted for each recipient with their respective public key.

B. *Authorization*

In addition to managing who can open a document, organizations gain additional protection through authorization. Authorization specifies what a user can do with a document and is achieved via permissions and dynamic document control

- Permissions govern a user's actions while working with a protected document. Permissions can specify whether or not a recipient who has access to the document is allowed to print or copy content, fill in fields, add comments or annotate the document, insert or remove pages, forward the document, access the document offline, digitally sign the document, and so forth.
- Dynamic document control maintains access rights and permissions assigned to an electronic document once it has been published and distributed. A document's author can make changes to a released document without having to manually redistribute it since the changes are automatically pushed to all existing versions of the document no matter where they reside. Using dynamic document control, organizations can manage and monitor electronic document use inside and outside the firewall, online and offline, and across multiple documents.

Dynamic document control includes the following capabilities:

- Document expiration and revocation—Post-publication document control can be maintained through the application of expiration dates and the ability to revoke access to a document. For example, an author can send a document that will expire in two weeks so that recipients will not be able to access it once the expiration date has passed. Or, access to a document can be automatically revoked if an authorized recipient leaves the project or changes departments.
- Offline access management—Organizations can manage how long an authorized recipient can access a document offline. Once the specified length of time has passed, the recipient can no longer view the document and must go back online to gain further access. Any access or permission changes that the author has made to the distributed document will be applied when the recipient goes back online.
- Persistent version control—Content and document management systems provide an effective mechanism for version control as long as a document stays within the confines of the system. Persistent version control expands on these capabilities by maintaining version control outside the system and offline. It allows document authors to make changes to a document's usage policies and prevent the obsolete version from being accessed while providing end users with the location of the updated version, no matter where the document resides.

Fig 3: Authorization is achieved via permissions and dynamic document control

C. *Accountability*

Document auditing allows organizations to maintain accountability with regard to the use of protected documents, because they can know precisely:

- How a recipient has used a document
- How often each type of usage occurred
- When that usage occurred

© 2014, IJCSMC All Rights Reserved

Accountability is achieved when an author can track each recipient's use of a document for each permission assigned (such as allowing a user to fill in fields on a form, print, forward, save a copy, and so forth.) Auditing should include automatic notifications about the use of protected documents. For example, a customer service representative sends a customer a time-critical electronic statement that requires an action on the customer's part, such as a reply or digital signature. Once the customer receives the electronic document, the representative is automatically notified when the customer opens it. If the customer fails to open the document, the representative is notified after 24 hours. Alternatively, a customer relationship management (CRM) system can leverage failure notification to initiate an escalation or specific follow-up task by the customer service representative.

IV. DIGITAL SIGNATURES

When enterprises distribute documents electronically, it is often important that recipients can verify:

- That the content has not been altered *(integrity)*
- That the document is coming from the actual person who sent it *(authenticity)*
- That an individual who has signed the document cannot deny the signature *(non-repudiation)*

Digital signatures address these security requirements by providing greater assurances of document integrity, authenticity, and non-repudiation [5].

A. Integrity

Digital signatures enable recipients to verify the integrity of an electronic document that is used in one-way or round-trip workflows. For example, when a digital signature is applied to a quarterly financial statement, recipients have more assurance that the financial information has not been altered since it was sent. Methods for maintaining integrity include:

- Parity bits or cyclical redundancy checking (CRC) functions—CRC functions work well for unintentional modifications, such as wire interference, but they can be circumvented by a clever attacker.
- One-way hash—a one-way hash creates a fixed-length value, called the hash value or message digest for a message of any length. A hash is like a unique fingerprint. With a hash attached to the original message, a recipient can determine if the message was altered by recomputing the hash and comparing his or her answer to the attached hash. Common hashing algorithms are MD5, SHA-1, and SHA-256. Electronic has adopted the SHA-1 and SHA-256 algorithms because of their wide acceptance as a security standard.
- Message Authentication Codes (MAC)—A MAC prevents an attacker from obtaining the original message, modifying it, and attaching a new hash. In this case, a symmetric key is connected to the MAC and then hashed (HMAC). Without the key, an attacker cannot forge a new message. Electronic uses HMACs where appropriate.

Fig 4: Digital signatures verify the integrity of an electronic document

B. Authenticity

Digital signatures provide document authenticity by verifying a signer's digital identity. For example, a digitally signed quarterly financial statement allows recipients to verify the identity of the sender and assures them that the financial information has not been altered since it was sent. Digital signatures are created using asymmetric key cryptography. For document encryption, a document's author encrypts a document using a public key. Because the recipient is the only person with the private key, he or she is the only one who can decrypt the message. Digital signatures reverse the use of public and private keys for document authenticity. The author encrypts the hash of the message with a private key. Only the public key can correctly decrypt the hash and use it to see if it matches a new hash of the document. Because recipients of the document have the author's public key, they gain greater assurances that the individual who signed the document was the person who encrypted the original hash.

- The process that constitutes a digital signature is as follows:
- A hash is created of the original document.
- The digital signature is created, which encrypts the hash with a private key.
- The signature is included with the document.

© 2014, IJCSMC All Rights Reserved

Electronic Acrobat supports multiple digital signatures placed anywhere in the document for proper presentation. In fact, Electronic Acrobat tracks all previously "signed" versions within the document for easy verification of changes made during the document's lifecycle. Furthermore, Electronic offers a certified signature, which is the first signature on the document. With a certified signature, the author can specify what changes are allowed for integrity purposes. Electronic Acrobat will then detect and prevent those modifications.

Fig 5: Digital signatures verifying a signer's digital identity

C. Non-repudiation

Non-repudiation is a document security service that prevents the signor of the document from denying that they signed the document. Support for this service is often driven by authentication and time-stamping capabilities.

D. Public key infrastructure (PKI)

Public key infrastructure (PKI) mainly provides a digital certificate that enables a document's recipient to know whether or not a specific public key really belongs to a specific individual. Digital certificates bind a person (or entity) to a public key. Certificate authorities (CA) issue these certificates and recipients must trust the CA who issued the certificate. X.509 is the widely accepted certificate standard that Electronic uses. If a certificate expires or a private key is compromised, the CA will revoke the certificate and record the revocation. As part of the process of authenticating a digital certificate, recipients can check the certificate's status. Certificate validity can be checked using the following standard methods:

- Certificate revocation list (CRL)
- Online Certificate Status Protocol (OCSP)

Electronic uses both CRL and OCSP. The following additional mechanisms can make up a PKI:

- Public-Key Cryptography Standards (PKCS)—a set of standard protocols for PKI used by multiple vendors. The standards include RSA encryption, password-based encryption, extended certificate syntax, and cryptographic message syntax for secure multipurpose Internet mail extensions (S/MIME).
- Registration authority—used to run background checks on individuals who wish to obtain a certificate.
- Certificate repository—repositories that house digital certificates.
- Key update, backup, recovery, and history—Mechanisms for key maintenance and archiving.
- Cross-certification—in the absence of a single global PKI, which is highly unlikely, this mechanism allows users from one PKI to validate certificates from users in another trusted PKI.
- Time stamping—a critical component of non-repudiation that offers a time stamp from a trusted third party.

Fig 6: Digital signatures address security requirements by providing greater assurances of document integrity, authenticity, and non-repudiation

V. CONCLUSION

The use of sensitive and mission-critical information in electronic processes is essential for thousands of businesses and government agencies. Document security solutions leverage standards-based techniques for document control and digital signatures to provide effective solutions that enhance the privacy and confidentiality of electronic documents and forms. With a comprehensive set of desktop- and server-based solutions, offers convenient, easy to use document security capabilities that encourage users to keep information private and help organizations meet the strictest regulations for sharing information electronically. The above explained security solutions enable organizations to replace paper-based business processes with

© 2014, IJCSMC All Rights Reserved

electronic processes to reap the benefits of improved operational efficiency, reduced costs, and increased customer and constituent satisfaction.

REFERENCES

[1] http://www.en.wikipedia.org/wiki/Digital_preservation
[2] http://www.en.wikipedia.org/wiki/six_key_criteria_for_providing_document_peristant_security
[3] https://www.gov.uk/data/NC_framework_document_-_FINAL.pdf
[4] http://www.en.wikipedia.org/wiki/Document_security
[5] Adrian Spalka, Armin Cremers, and Hanno Langweg. Protecting the Creation of Digital Signatures with Trusted Computing Platform Technology Against Attacks by Trojan Horse. In IFIP Security Conference, 2001

© 2014, IJCSMC All Rights Reserved