International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-6, June 2015

Improving the Security of Workflow-based System using Multiple Digital Signatures

Mayuri Anil Jain, Uday B. Joshi

***Abstract*— Private companies and Government Organizations all around the world make huge investments for the automation of their processes and in the management of the electronic documentation in recent times. The main requirement in the management of digital documentation is its equivalence, from a legal perspective, to paperwork, affixing a signature on a digital document is the fundamental principle; which are based the main processes of authorization and validation, apart from the specific area of application. Main benefits for introduction of digital signing processes are cost reduction and complete automation of documental workflow, including authorization and validation phases. In essence, digital signatures allow you to replace the approval process on paper, slow and expensive, with fully digital system, faster and cheaper.**

***Index Terms*— workflow based system; Certificates; USB Tokens; XML Digital Signature; Multiple Signatures.**

I. INTRODUCTION

Due to rapid development of technology, organizations are in the process of heading towards paperless environments. They have channeled their efforts to achieve this by adopting automation and by digitalizing paper documents through a series of techniques that include imaging, scanning and Electronic Document Interchange. The digital form of document enables easy management, circulation and makes it available anytime and anywhere by using Internet.

The main requirement in the management of digital documentation is its equivalence, from a legal perspective, to paperwork, affixing a signature on a digital document is the fundamental principle on which are based the main processes of authorization and validation, apart from the specific area of application.

Now-a-days, investment on system/data security in any organization has increased greatly, due to numerous attack threats lurking everywhere. So, Digital Signature is one of the many ways to authenticate the data at any point of time.
One of the major advantages of Digital Signature is that it ensures authenticity and integrity of data, which in today's date is of great importance.

From using traditional Digital Signature methods we have come a long way today to using XML Digital Signatures.

Mayuri Anil Jain, Computer Engineering, K. J. Somaiya College of Engineering,Vidyanagar, Vidyavihar(E), Mumbai - 400 077, Maharashtra.

Uday B. Joshi, Associate Professor, Computer Department, K. J. Somaiya College of Engineering, Vidyanagar, Vidyavihar (E), Mumbai - 400 077, Maharashtra.

W3C has introduced the syntax and promoted the usage of XML Digital Signatures.

II. RELATED WORK

The popularity and growth of Internet have been a driving force to make extensive use of technology to extend business operations with digitalization of documents. However the need has also been felt to maintain authenticity and security of information. A replay attack resilient mechanism was therefore required to embed digital signature into documents, along with a timestamp from authorized time stamping authority. The choice automatically falls on use of PKI technology, which is one of the most widely used key management schemes. In this paper we present a mechanism to sign electronic document with digital signature comprising of digital certificate and asymmetric key stored in cryptography token. Thereafter, the document gets time stamped from authorized third party timestamp server so that authenticity and time of creation can be verified and repudiation attack can be handled. The mechanism is also replay attack resilient. It ensures electronic documents are digitally signed with secure signature in order to maintain authenticity and genuineness.

III. FUNDAMENTAL CONCEPTS

A. How Digital Signature works

The private key of the originator is used as input to the algorithm which transforms the data being signed (or its hash value). This transformation can only be reversed, and the data decrypted and accessed, by use of the originator's public key, which is provided to the recipient(s) by the originator.

1) Creating a Digital Signature with Private Key

Data encryption using asymmetric keys is an expensive operation directly proportional to the size of the data being encrypted; it potentially doubles the size of the data increasing the processing power and bandwidth required to process and transfers the data. A more efficient approach is to first use a secure cryptographic hash function (such as SHA-1) which can take large objects of varying size and produce a unique fixed-size hash value or message digest. The much smaller hash value can then be encrypted with the private key of the originator to produce the digital signature.
Having calculated the message digest this can be encrypted using the private key of the originator to produce the digital signature, as shown in the diagram below:

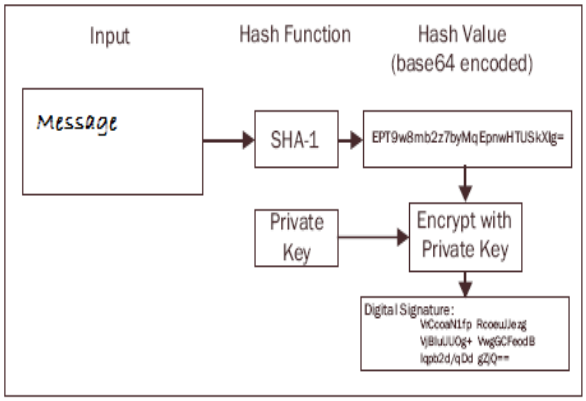

Figure 1 Creating a Digital Signature

2) Verifying a Digital Signature created with Private Key

The recipient must de-crypt the digital signature using the public key of the originator and recalculate the hash value of the corresponding digital object. If the calculated hash value does not match the result of the decrypted signature, either the object has been altered since being signed, or the signature was not generated with the corresponding private key of the originator.

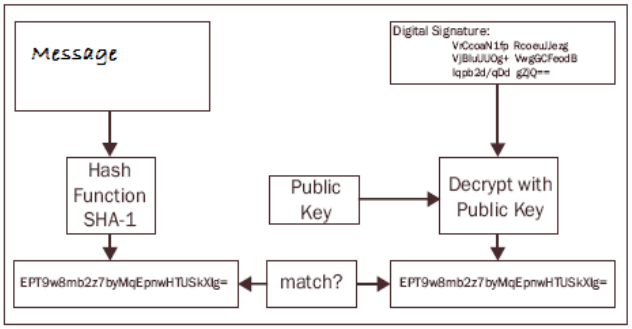

Figure 2 Verifying a Digital Signature

B. *XML Digital Signature*

XML signature is form of digital signature designed for use in XML transactions. The XML Digital Signature standard defines a schema that is used for storing the result of a digital signature operation applied to (in most cases) XML data [2]. Like non-XML digital signatures, XML signatures add authentication, data integrity, and support for non-repudiation to the data that is object of XML digital signing process. However, unlike non-XML digital signature standards, XML signature has been designed to both account for and take advantage of the Internet and XML.

A fundamental feature of XML Signature is the ability to sign only specific portions of the XML content rather than the complete document. This is relevant when a single XML document may have a long history in which the different components are authored at different times by different parties, each signing only those elements relevant to it. This flexibility will also be critical in situations where it is important to ensure the integrity of certain portions of an XML document, while leaving open the possibility for other portions of the document to change. Since data security – in form of data verification and authorization - represents an important part of information system security paradigm this article is addressing the questions and possibilities of XML Digital Signature usage in everyday information system security procedures.

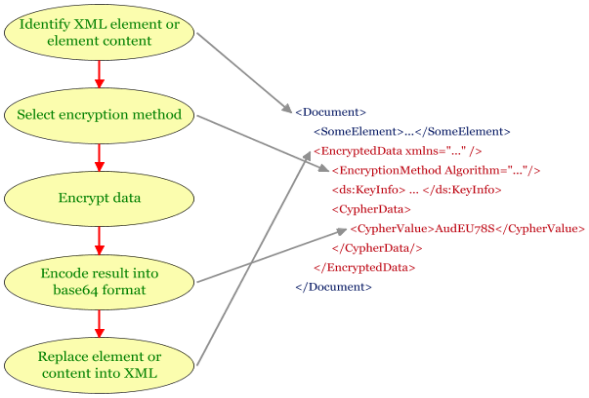

Figure 3 Flow of XML Digital Signature

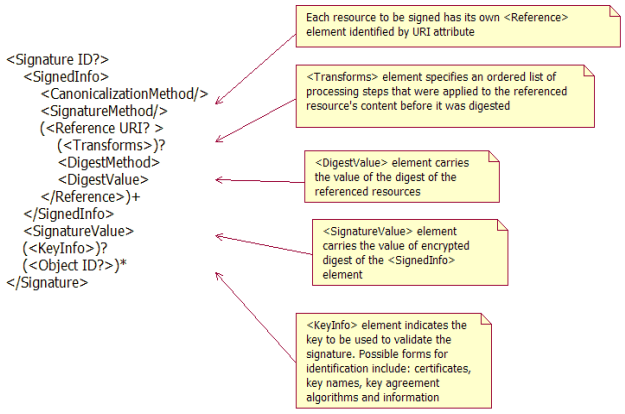

Figure 4 Format of XML Digital Signature

C. *Creating and verifying XML signatures using the W3C recommendation*

XML signature creation

In this example two digital objects are to be signed with a single digital signature:

- The Paradigm logo (http://www.paradigm.ac.uk/images/paradigm.gif).
- The Paradigm home page (http://www.paradigm.ac.uk/index.html).

1. For each object a <Reference> element is created containing:
   - The location (URI) of the object.
   - An ordered list of the transforms (or processing steps) that were applied to the content of the referenced resource before its digest was calculated.
   - The actual algorithm used (such as SHA-1) to calculate the digest value.
   - The digest value (base64 encoded) for the identified object in the <DigestValue> element.
2. These <Reference> elements are collected within the <SignedInfo> element along with:
   - The canonicalisation method (e.g. XMLC14N as used in the example below) to be applied to the <SignedInfo> element.
   - The signature algorithm to be applied to the <SignedInfo> element.

3. The <SignedInfo> element does not include explicit signature or digest properties (such as date or calculation time), if these are required they can be associated via a <SignatureProperties> element attached to an <Object> element.
4. The populated <SignedInfo> element is then canonicalised using the specified <CanonicalizationMethod>.
5. Finally the <SignatureMethod> which is a combination of a digest algorithm and a key dependent algorithm (e.g. DSA-SHA1) is applied to the canonicalised <SignedInfo> element and the digest result is placed in the <SignatureValue> element.

XML signature verification

The verification of an XML signature consists of of two phases:

1. Signature validation
   - This comprises the verification of the <signatureValue> of the <SignedInfo> element:
   - The digest of the <signedInfo> element is recalculated using the digest algorithm specified in the <SignatureMethod> element.
   - The public key from <KeyInfo>, or from an external source, is used to verify that the <SignatureValue> matches the recalculated <SignedInfo> digest.
2. Reference validation
   - This comprises the verification of the <DigestValue> of each <Reference> element
   - The <SignedInfo> element is canonicalised using the algorithm specified in <CanonicalizationMethod>.
3. For each referenced object in the canonicalised <SignedInfo> the recipient must:
   - Obtain a copy of the object.
   - Apply any transforms specified to the object.
   - Regenerate the digest for the transformed object using the <DigestMethod> specified in its <Reference> element.
   - Validation fails if the generated digest value and the <DigestValue> in the <Reference> do not match.

IV. PROPOSED SYSTEM

In this project we will be making use of XML Digital Signatures, but the format specified by W3C for XML Digital Signatures will not be followed. Instead customized XML Digital Signature tags will be used to implement Digital Signatures in Workflow Based System, where signature over signature (multiple signs) will be present on the single document.

The main purpose of Multiple Signature Based Incident Report Workflow system is to transmit the created reports electronically in a secure method within the hierarchy of the organization using Digital Signature infrastructure. Digital signatures let the recipient of the report (information) was not altered while in transit. The staffs have to manually create reports and hand in to the concerned higher authorities in the existing system. The process is awkward and time-consuming for all the concerned authorities as taking action against any incident which has occurred gets delayed. Technology to electronically submit the reports electronically is available. However, there do exist certain requirements such as the authenticity of the report and confirmation of the recipient. The organization also needs to be certain about the originator of the report and that the staffs cannot falsely claim not having sent the report.

We have also modified the regular Database design to accommodate the duplication of data required for Digital Signatures. XML Documents will be generated at runtime. Authentication and Integrity of data in workflow based system is achieved by attaching a Digital Signature at every stage of the workflow with the XML Document.

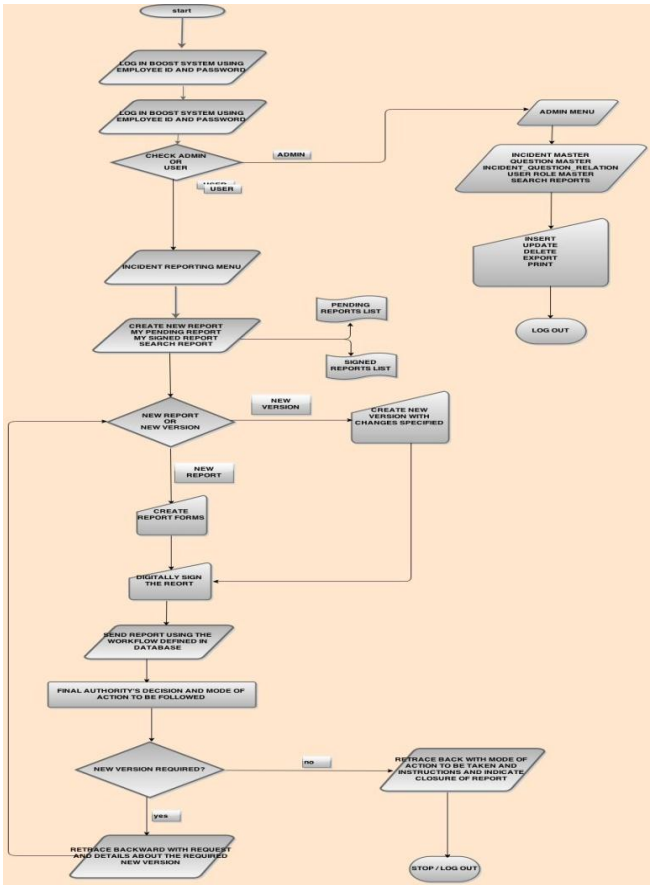

Figure 5 Flowchart of Project

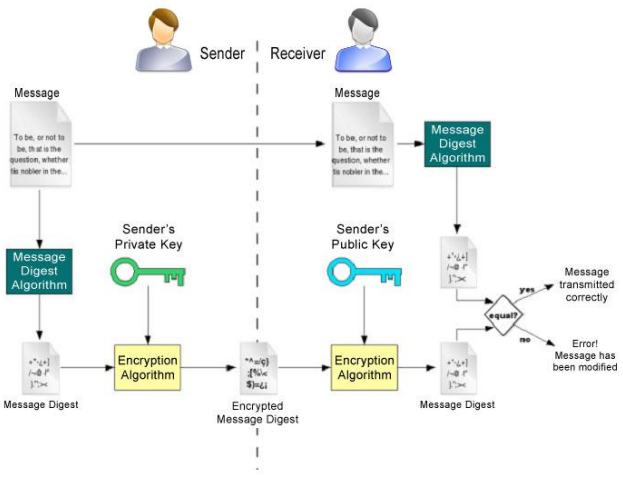

Figure 6 Lifecycle of Digital Signature

The current systems implementing multiple digital signatures are a thick client based application designed using JAVA language. But an attempt at creating a web based workflow application with multiple (hierarchal) signatures is being made. The web application is designed using PHP technology – GUI and JAVA Applet – signature API. The proposed system is an attempt at taking the current system from Intranet to Internet with concept of multiple signatures.

As in Fig. 1 the flow of the project is depicted. There are two parts in the project. One where the Admin controls the database and another where the actual implementation of Digital Signature will be made. The reports which will be created will be first signed by the creator, and then forwarded upwards in the hierarchy. Later on in the higher levels the employees can decide whether the report is to be reverted back for improvement, forwarded for what further action is to taken or locked (where the report will be closed and saved in the database). There will be minimum two signatures attached to a single report – one, of the employee who creates the report and other, will the one who will close the report with remarks and comments about the course of action that will be taken.

As the fig. 2 shows how a digital signature works in general, the process is followed in this application as well. The employees are given PKI USB Tokens [6] to store their private keys. The digital certificates are provided by the local Certificate Authority of BARC with the help of local Registration Authority of BARC. Then a XML file is created at runtime and shown to the user to ensure the "What You See Is What You Sign" context is taken care of [2]. The XML file contains all the data that been entered by the user before digitally signing the contents. Then the process explained in section 3 is followed.

V. Conclusion

Security threats in government organizations such as BARC, when an unauthorized party inserts counterfeit objects into the system can be eliminated through the system. There are various hacking tools available that can quite easily intercept online messages, who's content, unless encrypted, will be fully available to the attacker.

There are a lot of tools that let people send "spoofed" messages. These are messages that appear to have come from someone that user know, when in reality they were sent by the attacker trying to social engineer his way into the system. If all conversations with the people that user know and trust are digitally signed, user will easily identify that the message did not come from a true sender.

It is more efficient and makes the process of reporting become easier because once the employee repots an incident; it will be directly sent to the next concerned authority for further action to be taken. After the report has been sent to the next level, the employee can see the status of the report whether it has been taken care of or not. The employees do not have to do anything such ask the concerned officers to know the status but just wait until they receive any further instructions online. Employees can file a report no matter from anywhere as long as they have computer or tablet and have them connected to the Intranet. Employees do not need to anywhere to get the incident reporting form. Besides that, the reporting is done in a paperless environment. It means we do not need to use any paper for application.

The interface design of the application is in a systematic and attractive view. It has various windows control such as combo boxes or drop-down menus, proper prompts for errors are considered.

Acknowledgment

I would like to thank BARC guide Mr. D. K. Dixit, who has guided at every step of this project. Project completion could have been a challenge without his guidance and support.

References

[1]. Goswami, S.; Misra, S.; Mukesh, M., "A PKI based timestamped secure signing tool for e-documents," High Performance Computing and Applications (ICHPCA), 2014 International Conference on , vol., no., pp.1,6, 22-24 Dec. 2014

[2]. Soderstrom, H., "Self-Contained Digitally Signed Documents: Approaching "What You See Is What You Sign"," *Information Science and Applications (ICISA), 2014 International Conference on* , vol., no., pp.1,4, 6-9 May 2014

[3]. Ponnapalli, Harigopal K.B.; Saxena, Ashutosh, "A Digital Signature Architecture for Web Apps," IT Professional , vol.15, no.2, pp.42,49, March-April 2013.

[4]. Geric, S.; Vidacic, T., "XML digital signature and its role in information system security," MIPRO, 2012 Proceedings of the 35th International Convention , vol., no., pp.1520,1525, 21-25 May 2012.

[5]. Tao-Ku Chang; Te-Feng Chiu, "A Secure Web services-based workflow management system," Electric Information and Control Engineering (ICEICE), 2011 International Conference on , vol., no., pp.1108,1111, 15-17 April 2011.

[6]. Ali, A.M., "Seamless Fusion of Secure Software and Trusted USB Token for Protecting Enterprise & Government Data," Availability, Reliability and Security (ARES), 2011 Sixth International Conference on , vol., no., pp.409,414, 22-26 Aug. 2011.

[7]. Leung, K.R.P.; Hui, L.C.K., "Multiple signature handling in workflow systems," System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on , vol., no., pp.8 pp. vol.2, 4-7 Jan. 2000.

[8]. J. Schwartze; B. Haarbrandt; D. Fortmeier; R. Haux; C. Seidel, "Authentication Systems for Securing Clinical Documentation Workflows ", Germany, November 19, 2013.

[9]. Leung, K.R.P.; Hui, L.C.K., "Signature management in workflow systems," Computer Software and Applications Conference, 1999. COMPSAC '99. Proceedings. The Twenty-Third Annual International, vol., no., pp.424,429, 1999.

[10]. Definition Of RSA [online]. Available : http://searchsecurity.techtarget.com/definition/RSA

[11]. General Questions related to Digital Signatures [online]. Available : http://www.e-mudhra.com/faq.html

[12]. X.509 Certificate Standard [online]. Available : http://www.symantec.com/business/support/index?page=content&id=TECH179202

[13]. X.509 Certificate [online]. Available : http://ftp.sunet.se/pub/security/docs/PCA/misc/x509v3.pdf

[14]. PKCS#11 Document [online]. Available : https://vhome.offis.de/sibyllef/fast11.pdf

[15]. PKCS#11 Definition [online[. Available : https://www.opensc-project.org/opensc/wiki/PKCS11

[16]. Clulow, J.: On the security of PKCS #11. In: CHES'03. LNCS, vol. 2779, pp. 411–425. Springer-Verlag (2003).

[17]. Local Registration Authority [online]. Available : http://searchsecurity.techtarget.com/definition/registration-authority