Digital Signature Verification with Etoken Based Authentication in Local Area Network

Mr. Sandip Kumar Bala, Mr. Manoj Kumar Behera

Department of Master in Computer Application, College of Engineering Bhubaneswar, Odisha, INDIA.

ABSTRACT

In this paper, we suggest creating digital signatures automatically utilizing the recently created the Probabilistic Digital Signature Scheme (PDSS) digital signature technique in the templates with extra security features like E-Token based authentication, such as Microsoft Word, Excel, and PowerPoint. Two different cryptographic assumptions—Integer Factorization (IF) and Discrete Logarithm (DL)—will be used by this BS-PDSS technique. These days, security is more crucial in fields like the army, navy, and other defense applications. Our project is intended for use in highly secure local area networks, such as those used by the Army, Navy, and other defense applications. Even though there are other file formats available, Microsoft products are the ones that are most frequently utilized. Thus, we are putting forth this idea for Microsoft Word, Excel, and PowerPoint products. Both the document's originator and reader must authenticate themselves via the highly secure authentication within that local area network. Even if they are utilizing secure authentication, no digital signature is generated automatically when they create a document. Therefore, we are suggesting that the digital signature in the aforementioned products be generated automatically. Even though it is possible to sign the documents precisely, no one uses it these days. As a result, we have to impose the requirement that all signers use their digital certificates at the time of document creation. In order to prevent anyone other than authorized users from reading the documents, we are employing authentication for both the document's originator and reader. Even if our system is secured by a login, if a user logs out without changing anything, anyone can use your system to cause any kind of fault. Thus, this "E-Token based two-factor authentication" is what we are recommending. The user will be prompted to authenticate twice as a result. The first is while they are use the system. Afterwards, if they attempt to produce a new document.

Key Words: Discrete Logarithm, BS-PDSS, private key, Public Key

1. INTRODUCTION

Security is more crucial now days in sectors like the army, navy, and other defense applications. The most widely used file format, despite the fact that there are others, is one for Microsoft programs.Thus, we are putting up this idea in relation to Microsoft Word, Excel, and PowerPoint products. Both the author and the viewer of the document must authenticate themselves within that local area network using the extremely secure authentication.Whenever they create a document, a digital signature is not automatically generated, even though they are utilizing secure authentication. Therefore, we are suggesting that the aforementioned products generate digital signatures automatically. Even if there is a choice to specifically signing the paperwork—these days, no one uses that. Thus, we need to impose the requirement that everyone must create the document themselves and sign it using their digital certificates. In order to prevent anyone other than authorized users from reading the documents, we are employing authentication for both the document's originator and reader. Even though our authentication is based on system login, if a user logs off and leaves the system unattended, anyone can use it to perform any kind of malicious activity. Thus, we are putting out this two factor authentication based on E-Tokens_. The user will be prompted to authenticate twice as a result. One occurs each time they use the system. Afterwards, if they attempt to produce a new document.

GOAL

Our project's primary objective is to safeguard documents stored on local area networks by offering secrecy, authentication, and integrity. Availability and Non-Repudiation must be considered under the security heading.

2. APPLICATION

A. Design and implementation

This pluggable digital signature creation solution can be configured to function with any current or previous version of Microsoft Office. This indicates that the capability of automatically generating digital signatures is enabled for older versions as well. Here, we're use the PDSS method, which is a secure digital signature generating technique currently in use. The digital signature mechanism is embedded into Microsoft Word and Excel through the use of VBA (Visual Basic for Applications).Integrity, non-repudiation, secrecy, and authentication are features of the application. Microsoft Office uses RSA cryptography with SHA1, which is vulnerable to collisions. However, BS-PDSS shields the document from both simple and collision assaults.

B. RSA with SHA1

Microsoft Word, Microsoft Excel, and Microsoft PowerPoint are word processors that use SHA1 and RSA to generate digital signatures. SHA1 is a hashing method used for document and certification signing, while RSA is an encryption/decryption system used for secure communications. To begin with, it is undoubtedly not a terrible idea to stay away from SHA-1 since there are other algorithms that, as far as anyone is aware, do not have the SHA-1 vulnerabilities.

C. Our analysis on RSA with SHA1

SHA-1's security is dependent on how it is used by the user. An attacker can produce two input strings with the same SHA-1 hash using less processing power than would be required for a decent hash algorithm, which is known as collision vulnerability. He is not, however, given the freedom to choose which of those input strings to use, nor is it always possible for him to locate a string whose hash coincides with a specific string.

Collision assaults may be susceptible if the attacker has any control over whatever you are prepared to sign. Using the IF problem, Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) created the first widely used encryption and signature method in 1978. The deterministic feature of this program ensures that the same digital signature or ciphertext is obtained for the same message each and every time. The intractability of the RSA problem (the extraction of the eth root problem) and the hardness of the IF problem form the foundation of the signature scheme's security. There are two types of applications for the RSA signature scheme: message recovery and appendix. Because of its multiplicative nature, the appendix kind of application is both existentially and selectively forgeable and vulnerable to simple assaults. Thus, this article comes to the conclusion that these plans are forged. As a result, two highly well-liked digital signature schemes—the BS-PDSS Scheme—that use the DL and IF problems have been proposed. Integer multiplications determine the computational complexity (asymptotic running time) of IF and DL problems.

D. BS-PDSS scheme

An updated —BS-PDSS‖ utilizing IF and DP problems is presented in this section. Afterwards, two big k-bit (security primes (Sophie-Germian primes) $p = 2p\sim + 1$ and $q = 2q\sim + 1$ are chosen, and the composite modulus has the formula $N = pq$.

Next, an element $g \in Z * N$ (the generator of the group $Z *N$) with order $\lambda(N\}) = p\{q \}$ is chosen. Following the computation of $(g, N, \lambda(N\}))$, the following algorithm for BSPDSS is suggested.

1. *Algorithm: BS-PDSS*

I. Following the computation of $(g, N, \lambda(N\}))$ on the provided security parameter k, a random number $X \in Z\lambda(N\})$ is chosen, and the public exponent $Y = g X \bmod N$ is calculated. (N, Y, g) and $(N, X, g, \lambda(N\sim))$ are the pairs of public and secret exponents, respectively.

II. The signature signing procedure uses a secret exponent $(N, X, g, \lambda(N\}))$ to compute a signature pair $(\sigma 1, \sigma 2)$ for message M, where an integer $k \in Z\lambda(N\})$ is chosen at random. This is done so that $\sigma 1 = g k \bmod N$ and $\sigma 2 = k -1 (M - X) \bmod \lambda(N\})$.

III. Using the public exponent (N,Y,g) of the signer for input message M, the signature pair $\sigma 1 = g k \bmod N$ and $\sigma 2 = k -1 (M - X) \bmod \lambda(N\})$ are verified by computing $V1 = g M \bmod N$ and $V2 = (Y \sigma 1 \sigma 2) \bmod N$. After that, it is determined that if V1 == V2, accept; if not, reject.

E. **Etoken based Authenication**

The security tool known as Etoken solves the authentication problem.The private key associated with each unique user is contained in eTokens. The E-tokens use the Crypto standard and are USB-based gadgets. Typically, certificates, private keys, and public keys are needed for PKI operations. The E-token always keeps private keys safely saved. E-token stores certificates since it makes mobility possible.Setting token policies and carrying out standard token administration tasks are made possible by EToken. Moreover, E-Token offers administrators and users a rapid and simple method for transferring digital keys and certificates. E-Token Properties comprise a password quality feature that establishes parameters to compute an E-token password quality rating, as well as an initialization feature that enables administrators to initialize tokens in accordance with certain organizational requirements or security modes.

It is forbidden to take an E-token out of the USB port while a procedure is underway. Multiple steps are needed for many tasks, including certificate selection, authentication, document signing, etc. It could be necessary to reinitialize the token's data structure if it is removed during one of these operations. The recipient(s)' public key certificates must be on file and correctly installed on the client PC. It is not possible to extract the private key from the E-token by just plugging it into a USB port.It is coded and used following the appropriate authentication process.

3. CONCLUSION

This paper introduces a new security feature that strengthens the security of the secure local area network, protecting the documents from forgeries and illegal access. This will give all of the papers on the local area network the standard level of protection.

4. REFERENCE

1.Shailendra Kumar Tripathi and Bhupendra Gupta, ―An Efficient Digital Signature Scheme by using Integer Factorization and Discrete Logarithm Problem‖ 978-1- 5090-6367-3/17/$31.00 ©2017 IEEE
2. R.Surendiran,Dr.K.Alagarsamy,"Skin Detection Based Cryptography in Steganography (SDBCS)",(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4) , 2010,ISSN: 0975 - 9646, Page 221 - 225.
3. Rishikant Sagar, Akhilesh Pandey,"A System for Verification of Offline English Signature Using Soft Computing Approach",International Journal of Computer Science and Engineering (SSRG-IJCSE),Volume-2 Issue-9 2015.
4. Surendiran.R, Rajan.K.P, Sathish Kumar.M,"Study on the Customer targeting using Association Rule Mining",(IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 07, 2010,ISSN: 0975-3397, Page 2483 – 2485 Rakesh Shukla, Hari Om Prakash, R.PhaniBhushan, Signature with Two Factor Authentication‖ 978-1- 5090-5769-6/16/$31.00 ©2016 IEEE
5. RakeshShukla, Hari Om Prakash, R.PhaniBhushan, Signature with Two Factor Authentication‖978-1- 5090-5769-6/16/$31.00 ©2016 IEEE [7] Dr.R.Surendiran,"Development of Multi Criteria Recommender System",International Journal of Economics and Management Studies (SSRG- IJEMS),volume4 issue1 2017,ISSN: 2393 - 9125,Page 28 - 33.
6. R.Surendiran,Dr.K.Alagarsamy,"A Crtitical Approach for Intruder Detection in Mobile Devices",International Journal of Computer Science and Engineering (SSRG-IJCSE) – Volume1 Issue4 2014,ISSN: 2348 – 8387, Page 6 - 14.
7. Haritha Damarla,"Research Methodology on Offline and Online Signature Verification and Forgery Detection",International Journal of Computer Science and Engineering (SSRG-IJCSE), Volume-4 Issue-11 2017.
8. S.Goldwasser, S. Micali, and R. L. Rivest, ‖A digital signature scheme secure against adaptive chosen- message attacks,‖ SIAM Journal on Computing, vol.17,no.2,pp.281–308,198 [11] Amit Kishore Shukla, Shreyas Singh,"Offline Signature Verification System using a Set of Simple Shape Based Geometric Features ",International Journal of Computer Trends and Technology (IJCTT),Volume-4 Issue-4 2013.
9. P. Kumar and B. P. Dungdung, ‖An extension of elgamaldigital signature algorithm,‖ Ph.D. dissertation, 2012.