IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 82-86
www.iosrjournals.org

Digital One Time Proxy Signature Using Domain Keys Identified Mail (Dkim) In Cryptography Under Network Security

K. Nirmala Devi[1]
[1] *(CSE, TejaaShakti Institute of Technology for Women, India)*

ABSTRACT:*One-time proxy signature scheme is a method for constructing a digital signature. Digital signature of a document is a piece of information encrypted by the signer's private key.Proxy signature is a digital signature where an original signer delegates her signing capability to a proxy signer, and then the proxy signer performs message signing on behalf of the original signer.Here, we propose two one-time proxy signature schemes with different security properties using Domain Keys Identified Mail where the domain name, the list of covered fields, the signing algorithm, and the method by which text snippets are simplified for signing purposes. In olden days.Other existing one-time proxy signatures are constructed from public key cryptography, From a verifier point of view, signatures generated by the proxy are indistinguishable from those created by the primary signer, a trusted authority can be equipped with an algorithm in public key cryptography our schemes are based one-way functions without trapdoors and so they inherit the communication and computation efficiency and complexity from the traditional one-time signatures. By using Domain Keys Identified Mail that allows the authority to settle differentiate between the signers. In our constructions, we use a combination of one-time signatures, oblivious transfer protocols using Domain Keys Identified Mail and its likely to make some kinds of phishing attacks easier to detect. We characterise these new protocols for DKIM and present constructions for them.*

Keywords-*Proxy signature scheme**,** Domain Key Identified Mail, one way function, primary signer ,oblivious transfer protocol,*

I. INTRODUCTION

Digital signature is a mathematical appearance of electronic kind of mark that gives the authentication about the sender's message which is not altered during transmission by third personality such as eve's dropper. It on the whole second-hand for software distribution, monetary transactions, and to noticecounterfeit. It is a type of asymmetric cryptography. It provides the non-repudiation import that the signer cannot successfully claim they did not sign a message. It consists of three algorithms such as key generation, signing algorithm, verifying algorithm. Digital signature is divided into two major types. One idea is one/multiple-time signature schemes which provides one signature per message (examples such as Rabin, Lamport, and rohatgi).The second idea is that public key cryptography where the same sign is used for multiple message protection (examples such as RSA and the ElGamal).Digital signature scheme **DS=(K,sign,VF).**

One-time signature was projected by Rabin and Lamport and is based on the initiative of committing public keys to secret keys using one-way functions.For more than 25 years, various variants of Rabin's schemes have been projected and investigated by many researchers. One time signature is whispered that Lamport signatures with large hash functions would at rest be protected in that event.the one time signature is

Pr (vk;sk) Gen [hFSignsk(_)(vk) forges] <=negl(n). One-time signature schemes have found abundant applications: in common on-line/off-line, and forward-secure signatures. In recent times, they have been used in multicast and broadcast authentication.

One advantage of one time signature is that fast verification and short signatures. It allows the signature of only a particular message using a given piece of private or public in rank. The same key pair can be used to authenticate multiple documents (paradigm Merkle Tree Signature Scheme). In modern days, one-time signatures have fascinated more and more attention, as an smart alternative to

the habitual signatures based on public key cryptography. With their confidence it can be implemented using fast hash functions.

Proxy signatures allow a elected person, called a proxy to sign in its place of a primary signer. A proxy signature adjusts a verifier that the primary signer has delegated the signing power to the proxy. To our acquaintance,all the formerly available proxy signatures are based on public-key cryptography.To identify our proxy signatures, we employ two basic cryptographic primitives .The first one is one-way functions without trapdoor. The second proposal is oblivious transfer protocol but both these method uses Domain Key Identified Mail (DKIM) to track the lane of signer by using header such as from, body, subject. By using this DKIMverifier will get the public key and then matches with the primary signer key. We confer constructions for the preferred proxy patterns, using polynomials over finite fields and error-correcting code.The rest of section co-ordinates as follow. In Section 2, we commence a model of one-time proxy signatures. In Section 3, we think about candidates for the blocks for construction of one-time proxy signatures. In Section 4, we offer a simple scheme for one-time proxy signatures using DKIM .In Section 5, we analysis the basic scheme and its security against attacks. In conclusion, Section 6 concludes the paper

II. MODEL OF ONE-TIME PROXY SIGNATURE

A primary signer gives his signing capability to proxy signer, so it generates his sign on behalf of primary signer. There are three type of classes of delegation which are full delegation, partial delegation and delegation by warrant. in full delegation proxy signer and primary signer have the same secret key for signing and verifying process, it doesn't provide non-repudiation, in partial delegation primary signer gives his/her authority to proxy signer so that proxy signer acts on behalf of primary signer, they have different keys, it provides non-repudiation, in delegation by warrant it gives more security by guarantee. it enables only by two signatures.

Here we proposed an full delegation method with domain key identified mail to track the path of primary signer.in this private key of proxy signer is derived from private key of primary signer. One time proxy signature uses only one key for both signing and verifying algorithm with two parties such as primary signer and proxy signer with three algorithm.

2.1.Signing algorithm:For an input, it consists of a message to be employed with private key of the signer, outputs a valid signature.forsigning,**s<-sign $_{sk}$(M).**

Algorithm:

$SIGN_{N,p,q,d}$(M)
If M belongs to group z return 1
Return M^dmod n.

2.2Verifying algorithm: for an output, he should use the same private key to open the message, if not it will show some message as not accepted or rejection.forverifying,**d<-VF_{mk}(M,S).**

Algorithm:

$VF_{N,p,q,}$(M,Q)
If M or Q belongs to group z return 0
Return M=Q^dmodn.return 1 else 0

2.3.Traceability: By using domain key identified mail we can trace the path of primary signer from proxy signer.it provides the id of primary signer.

Alice generates *(pk,sk)* **Bob has correct pk**

In olden model public key cryptography ,for signing and verifying uses public key to open the message, but in our onetime proxy signature using domain key identified mail full delegation technique is used such as both uses same private key to open the message and can able to track the path of particular signer.

III. CANDIDATES FOR THE BLOCKS FOR CONSTRUCTION

In this we took two models for constructing the models.

3.1.One time signature: in this Rabin introduced a technique for onetime signature where primary and proxy signers are interactive with one-way function, whereas Lamport uses non-interactive one time signature using digital sign with one way function. In our one time proxy signature defined as follows, let a,b,c be integers such that($^{b}_{c) >=2}$ ^{a}and let T be set from(1,2…b) and T_c be family of set and S denotes the mapping from T to T_k .here f is the one way function on S with security. With this security the secret key of **PK=(s1,s2….s_a),**and they keep the private key as secret and publishes the public key such as **PK=(v1,v2…v_a),**here **v1=f(s1),v2=f(s2)….v_a=f(s_a).**to verify the same thing reverse is applied.In Rabin algorithm the time complexity is **O(ab $\log^2$ a).**

3.2.Oblivios transfer protocol: A standard protocol is used between the sender and receiver and the goal of this is to send knowledge about string to receiver but the sender don't know which part is read by receiver. The sender has some secrets to disclose to receiver R.and the R should not reveal it. Let *g* and *h* be two (public) generators in a *q*-order group *Gq*, where *q* is prime. Assume that the secret input of *S* is ***p*1,p2, . . . ,*pn*∈*Gq*,** and the choice of *R* is α**, $1 \leq \alpha \leq n$.**the protocol follows as

1.S randomly selects n elements m_i and **S->R :(g^{m}_{i},f^{m})$_i$where f^{m}_{i} is ($m_i(y_i/h_i)$).**

2**.R->S:Y=g^{r},h^{a}**. for random r.

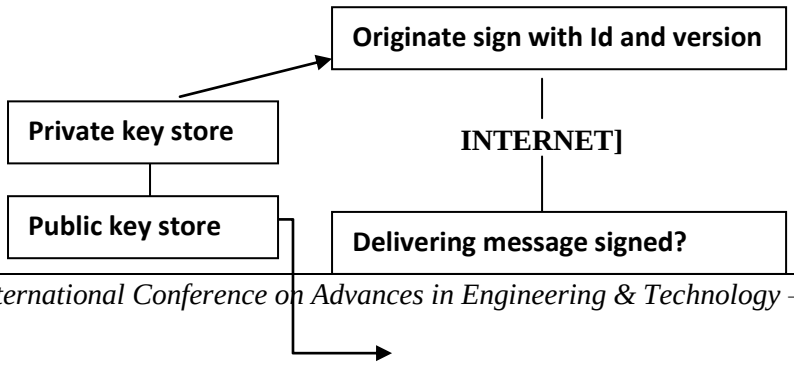
IV. ONE TIME PROXY SIGNATURE USING DKIM

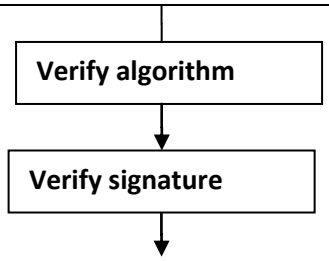
DKIM is a process for associate a domain name with an email message, in that way allowing a person to claim some task for the message. It is used for both signing and verifying process, in signing process it acts as an "author". DKIM normally uses header field such as "tag=value".in tag it uses "v" for version,"c" for canonical algorithm,"q" for query,"l" for length of c,"t" for timestamp,"x"for expire time,"b" for body,"bh" for body hashing,"s"for selector,"d"for domain. The default authentication is based on RSA.the signature is based on the following,

DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
h=from:to:subject:date:keywords:keywords;
bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
VoG4ZHRNiYzR

The primary signer generates n private or public keys say (sk1,pk1),(sk2,pk2)….(skn,pkn)for one time sign and publishes this keys as public key .within this receiver chooses one key as private key but proxy signer don't know which key was selected by receiver to open message. The proxy signer have sk_i private key to verify the DS. The digital signature send by proxy signer should be same as the receivers private key, if not it will not open.

The DKIM signature spread over header and body and both creates a different hash function.the signer uses the private key for digital signature. After a message has been signed by the signer an agent in the path can verify that it come from the original primary or proxy signer by using the id and version of the signer.





ACCEPT/REJECT

To thwart unprincipled by signers, a tracing algorithm has to be carefully considered and which should be run by a trusted authority.The oblivious transfer enables us to identify the true signer. In olden days,To do this, the trusted authority always asks the proxy to sign the disputed message again. Today's technology by using DKIM it is easy to track the path by using the id,version and body.If the proxy is unable to crop a dissimilar signature it means that either the proxy or primary signer really signed the message has applied the same secret key as proxy.

4.1.Proxy sign pattern

4.1.1.Key generation:

- The primary signer randomly chooses an m*narray S= $(sij)_{m*n}$as her private key. Each row holds nsecret keys of an instance of the one-time signature . The public key is $V = (vij)$m*n, where $vij = f(sij)$ and f is the one-way function.
- Oblivious transfer protocol is used stuck between the primary and proxy signer and at the completion of the proxy signer learns one secret key.
- The proxy signer compares it with primary signer whether the produced one is right or not**.(pk,sk)<-k**

4.1.2.Signing algorithm:

For an input, it consists of a message to be employed with private key of the signer, outputs a valid signature**.** For signing S<-**sign $_{sk}$(M).**

4.1.3.verifying algorithms:

for an output, he should use the same private key to open the message, if not it will show some message as not accepted or rejection. For verifying**<-VF_{mk}(M,S).**

To decrease the successful cheating we can increase the parameter n.the series of patterns can be generated as $(a_1,g1(a1))$,(a2,g2(a2))… $(a_i,g_i(a_i))$.Only 92.3% of observed signatures were successfully verified.

V. ANALYSIS THE BASIC SCHEME AND ITS SECURITY AGAINST ATTACKS

Suppose if the primary signer has the valid signature produced by proxy signature he/she can use the private key of proxy signature for next process.in order to protect this the key produced by proxy signer should be too many pair keys.

5.1. Key-only attack: in this the eve's droppers have permission to attack only public information of primary signer. The third party has to nearness the other side person that the message signed by the primary signer.

5.2. Known –message attack: in this eve has access one or more signature pairs otherwise she has permission to access some previously signed messages.

5.3. Chosen-message attack: in this eve makes primary signers sign one or more message for her. He has access to chosen text and later he creates forge sign of primary signer.

VI. CONCLUSION

In this we learned one time proxy signature. Unlike the olden cryptography which uses public key concept we proposed new model for one time sign with one way function.Eventhough it uses full

delegation it was not provide the primary signer path,but by using Domain Key Identified Mail (by id, version) it is easy to find the original primary signer. If there is any dispute between primary and proxy signer it calls the verifying algorithm to check whether the proxy and primary signer sign is same or not. If the signature is same it will send the acknowledgment of original sign, otherwise the proxy will generate the signature till the primary signer sign matches it.

One time proxy signature is basically used for fast signing and verifying algorithm. . It allows the signature of only a particular message using a given piece of private or public in rank. It consist of authentication of streams of packets in a distributed environment with mirror servers generating proxy signatures.

Our methodology is based on a combination of definite type of existing one-time signature with Domain Key Identified Mail technique. While the prior can be raised using the known procedures in the works, the concluding are new Domain Key identified Mail we introduce in this paper and so are of independent interest. In specific, the structures of strong proxy patterns are far away from clear, and as long as efficient constructions for them is a thought-provoking research problem.

VII. ACKNOWLEDGEMENT

This work is in part supported by Tejaashakthi institute of technology for women, india.

REFERENCES

[1]M. Abdalla and L. Reyzin. A new forward-secure digital signature scheme, Advancesin Cryptology { Asiacrypt'00, LNCS, 1976(2000), 116-129.
[2] J. N. E. Bos and D. Chaum. Provably unforgeable signature, Advances in Cryptology{ Crypto'92, LNCS, 740(1993), 1-14.
[3] M. Bellare and S. Micali.How to sign given any trapdoor function.Journal ofCryptology, 39(1992), 214-233.
[4] C. Dwork and M. Naor. An e±cient existentially unforgeable signature scheme andits applications, Advances in Cryptology { Crypto'94, LNCS, 839(1994), 234-246.
[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discretelogarithms, IEEE Transactions on Information Theory. 31(1985), 469-472.
[6]Y.-C Hu, A. Perrig and D.B. Johnson. Packet Leashes: A defense against wormholeattacks in wireless Ad Hoc Networks. Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003),2003, to appear.
[7] A. Hevia and D. Micciancio.The provable security of graph-based one-time signatures and extensions to algebraic signature schemes.Advances in Cryptology {Asiacrypt'02, LNCS, 2501(2002), 379-396.
[8] H. Kim, J. Baek, B. Lee and K. Kim. Secret Computation with secrets for mobileagent using one-time proxy signature.The 2001 Symposium on Cryptography andInformation Security, Oiso, Japan.
[9] B. Lee, H. Kim and K. Kim. Strong proxy signature and its applications.The 2001Symposium on Cryptography and Information Security, Oiso, Japan.
[10] M. Mambo, K. Usuda and E. Okamoto. Proxy signatures: Delegation of the powerto sign messages. IEICE Trans. Fundamentals, Vol. E79-A (1996), 1338-1353.
[11] R.C. Merkle. A digital signature based on a conventional function. Advances inCryptology { Crypto'87, LNCS, 293(1987), 369-378.
[12] M. Naor and B. Pinkas.E±cient oblivious transfer protocols.SODA01, 2001.
[13] H. Niederreiter and C. P. Xing, Rational Points on Curves over Finite Fields:Theory and Applications, Cambridge University Press, LMS 285, 2001.
[14] A. Perrig. The BiBa one-time signature and broadcast authentication.Eighth ACMConference on Computer and Communication Security, ACM, 2001, 28-37.
[15] M.O. Rabin. Digitalized signatures.Foundations of Secure Communication, Academic Press, 1978, 155-168.
[16] R.L. Rivest, A. Shamir and L. Adleman. A method for obtaining digital signaturesand public key cryptosystems.Communications of the ACM, 21(1978), 120-12.
[17]Crocker, D.; Hansen, T.; Kucherawy, M. (September 21, 2011). "DomainKeys Identified Mail (DKIM) Signatures". *Draft Standard.* IETF. *"Verifying the signature asserts that the hashed content has not changed since it was signed and asserts nothing else about "protecting" the end-to-end integrity of the message."*
[18]"STD 76, RFC 6376 on DomainKeys Identified Mail (DKIM) Signatures". IETF. *11 July 2013*. Retrieved 12 July 2013. *"*RFC 6376 *has been elevated to Internet Standard."*
[19] R. Rivest and A. Shamir. PayWord and MicroMint: two simple micro paymentschemes. Tech. Rep., MIT Lab. for Computer Science, 1996.
[20] W-G Tzeng. E±cient 1-out-n Oblivious Transfer Schemes. PKC'02, LNCS, 159-171