A New Hierarchical Signature Scheme With Authorization

Alper UĞUR, İbrahim SOĞUKPINAR

***Abstract* — Management and access control of data in a workflow system had an increasing trend with the improvement of information technology. Electronic signature implementations on workflow documents provide rapidness to the transactions and guarantees a certain security level as far as the signature scheme possesses. Unfortunately, in practice, it is not as easy as it sounds.**

Most of the organizations have hierarchical structure composed of departments with different levels. The levels of departments are defined by means of security required and services provided. Some departments would not have adequate rights on affirming/approving a specific document and this will eventuate as a problem of signature authorization of documents in a workflow.

We have proposed a new hierarchical signature scheme as a solution for the signature authorization problem mentioned above. The scheme is based on association of the authorization information with the signature where the new signature key is derived from the already employed key.

***Index Terms*— authorization, hierarchical signatures, signature schemes**

I. Introduction

Information and communication security is within the basics of advanced information systems. In these systems electronic signature applications substitutes traditional handwritten signatures to support security services and expedite the document workflow.

In a hierarchical organization, security must be one of the basic requirements for access control and management of all processed documents in workflow. Electronic signature deals with the documents in case of authorization, authentication and integrity.

In this paper, we focused on problems of electronic signatures in hierarchical organizations as a hierarchical signature where the organizational level of the signer is important. It is the access control level in the document workflow or an affirmation right of documents within a hierarchical order.

In digital environment, any signer could approve and sign a document with his/her secret signature key. As traditional we may check its corresponding public key if it is a known signature in the organization. Would the verification of a signature on a document be adequate to prove the "validity" of the document?

Will this confirmation on the document acceptable if the signature was verified? How could the verifiable signature differentiated from authorized and verifiable signature?

In another case, an authorized person could be appointed to another/upper level/class in the hierarchical organization. It is obvious that his/her previous approval rights on documents in the organization workflow will be expanded and varied. In this case, if there was a predecessor, it must be ensured that he/she could not sign the documents in workflow anymore. Moreover, signature of the successor -the new authorized person- must be proclaimed to the hierarchical structure, as it is valid and verifiable on these level documents.

Changing signature keys seems as though practical for the given cases above. Nevertheless, this operation will trigger the new key generation, insertion operations and revocation operation on old key. However, the challenging key management operations in big organizations would be more complex even if they also have a hierarchical structure. Key replacements may affect the entire large key tree in the organization and causes remarkable computation cost [1].

Regarding to the cases above, the authorizations of different security levels/classes/duties in the hierarchical organization are the effective causes of signature variations. Considering this, we have purposed a new hierarchical signature scheme. The scheme associates the new authorization/position information to an already employed one to generate a new "authorized" signature.

This paper is organized as follows; In Section II, we give background information. In Section III, we describe the new hierarchical signature scheme. In Section IV, we presented the "authorized" signature implementation with XML Signature syntax developed for mobile and web environment. In Section V, we examine the scheme under security and efficiency aspects, and in the last section, we conclude the paper.

II. Background Information

Understanding the term "hierarchy" will be a good starting point while dealing with signatures in hierarchical structured organizations.

We could define "hierarchy" as the ranking or classification of individuals in an organization vertically or horizontally with respect to their duties or clearance. In a hierarchic organization the departments those form the organization would have

A. Uğur is with the Gebze Institute of Technology, Computer Engineering Dept. Information Security Lab. (e-mail: augur@ bilmuh.gyte.edu.tr).

İ. Soğukpınar is with the Gebze Institute of Technology, Computer Engineering Dept. (e-mail: ispinar@ bilmuh.gyte.edu.tr).

distinct levels according to their relationship and duties. Some departments would not have adequate rights on affirming/ approving a specific document and some documents in hierarchical workflow have to be processed with a sequential order between levels.

The hierarchy in an organization is formed with different ranks and security/authorization levels within defined vertical relationship. From bottom to up, the security requirements, authorizations and level of clearance will increase. In Fig. 1, organization of an army is given to demonstrate the hierarchical structure. At Level Zero, privates are the inferior authorities in the hierarchy but at the top generals have the complete authorization and the documents at this level must have high confidence.

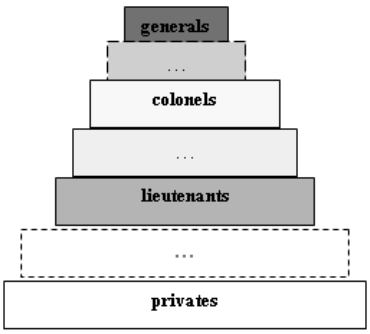

Fig. 1. Army as an example for the "hierarchical structure".

In this paper, we focused on problems of electronic signatures in hierarchical organizations as a hierarchical signature. The structure of a hierarchy will clarify the elements of a hierarchical signature: the levels, authorities and duties of classification and of course the signatures of individuals/people in the organization.

In previous section, we discussed the authorization of signature problem in a hierarchical organization. We also discussed a transformation of old signature with the authorization as a solution. This proposal is based on association of the authorization/level information with the signature.

The cases mentioned before must not be mixed up with the cases in proxy signature[2],[3],[4] or delegated signatures [5],[6],[7],[8],[9] in literature. These schemes are based on the case that a person/an agent or a group can sign on behalf of another person. However, in the hierarchical signature problem of signing a document behalf of another individual is not the case. The problem is temporary or permanent assignment of a person to a specific level of authorization who also belongs to a certain level in the same hierarchy.

There were also pretty researches on key schemes based on additional information called as "self-certified public keys" and "id-based signatures". In those structures, key/signature has informative, person specific ID data as name, surname, e-mail address that may help to verify the person [10],[11],[12].

In our scheme, the additional information is not concerning directly the person or not person-specific, it deals with information about authorization of signature. While the ID in above schemes must be a distinctive property of a person and unique, the additional authorization information associated with electronic signature in our hierarchical scheme may belong to more than one person if they have the same security level in the hierarchy.

In 2001, Boneh and Franklin [11] suggested an Id-based encryption scheme with Weil and Tate pairings on elliptic curves. It is the first practical, efficient and provably secure identity based encryption scheme based on pairings. The various threshold, ring, etc. signature schemes based on pairings were presented in the following years.

In 2002, Paterson [13] presented an id-based signature scheme with pairings over ElGamal scheme, in 2003 Cha-Cheon [14], purposed a scheme on pairings with gap Diffie-Hellman groups. Thereafter, C.-Y.Lin et al. [15] presented a group signature scheme based on Cha-Cheon's scheme.

Cha-Cheon's scheme is based on an id-based crypto system that a system administrator is responsible to set up operations. We adapted Cha-Cheon's scheme to act as a self-sufficient scheme that a person can generate his/her verifiable hierarchical signature associating his/her authorization information with the signature without any third party requirement. An exterior verification of authorization protocol is appended to the scheme to provide instant and later on verifications.

III. THE NEW HIERARCHICAL SIGNATURE SCHEME

In this section, we give the key and signature generation, signature and authorization verification phases of the scheme. We use the same notation and parameters as in [11], [14].

The parameters are:

S_i : signature of *i* in organization
h : information of hierarchical authorization
S_h (S_i,h) : Hierarchical signature
$(S_{i\text{-}pub}, S_{i\text{-}prv})$: the private and public keys of individual *i*
P : generator of gap DH group G_1
n : $n \in Z^*_q$ nonce
m : message
L_m : derived authorization level of message m
$H_1:\{0,1\}^* \rightarrow G_1$, $Hc:\{0,1\}^* \times G_1 \rightarrow Z^*_q$: cryptographic hash functions

$P \in G_1$ and $e(P,P)=1$
$S_{i\text{-}prv} \in Z^*_q$, $S_{i\text{-}pub} = S_{i\text{-}prv}.P$ (1)

Hierarchical signature key generation:
$S_{h\text{-}key}=S_{i\text{-}prv}.H_1(h)$ (2)

Hierarchical signature generation:
$R=n.H_1(h)$, $r=H_c(m,R)$ ve $S_h=(n+r).S_{h\text{-}key}$ (3)

Hierarchical signature will be: (S_h,R)

Hierarchical signature verification:
m, (S_h,R), $H_1(h)$
the authorization information are sent in clear text.

Calculate : $r = H_c(m,R)$ (4)
Verify the authorization : $H_1(h)$ (5)
Verify the signature : $e(P,S_h) = e(S_{i\text{-}pub}, R+r.H_1(h))$ (6)

The new hierarchical signature is generated with the $S_{i\text{-}prv}$ using (1), (2) and (3), the private key of *i* and signature verification is done with already known $S_{i\text{-}pub}$, the public key of *i* using (4), (5) and (6). In order that, there is not any demand for updating the hierarchical key tree or addition a new cryptographic key pair to it.

Contents of *h* the authorization information will be the authorization/duty and validity time interval in case of representative assignment.

The verification of authorization phase in the scheme can be operated with a tiny protocol in (7) between upper level and the signature verifier in signature verification phase and in interrogation of archived documents at any time.

Verification of authorization protocol:
Signature verifier Unit on upper level
"authorization verifier"

$E_{s\text{-}key}(S_{i\text{-}pub}, L_m)$ ----------→ h_i of $S_{i\text{-}pub}$ (7)
←---------- $E_{s\text{-}key}(H_1(h_i))$
$H_1(h_i) =? H_1(h)$ // $E_{s\text{-}key}$ session key encryption
authorized or not //can be cancelled if high level
//security is not required

IV. AUTHORIZED XML SIGNATURE

In this section an authorized signature is implemented with XML Signature syntax. XML Signature is a joint standard of the IETF and the W3C for digitally signing all of an XML document, part of an XML document, or even an external object. The XML Signature standard [16] is one of the main building blocks for Web Services Security [17]. In Fig. 2 the basic syntax of an <*Signature*> is given.

```
<Signature ID>
        <SignedInfo>
                <CanonicalizationMethod/>
                <SignatureMethod/>
                (<Reference URI?>
    (<Transforms>)?
                        <DigestMethod>
                        <DigestValue>
                        </Reference>)+
        </SignedInfo>
        <SignatureValue>
        (<KeyInfo>)
</Signature>
```

Fig. 2. XML Signature Syntax

The authorized signature can be implemented with *SignatureProperties* element which is already defined in standards [18]. The *SignatureProperties* element can be used to encapsulate information about the signature itself.
We embedded the authorization information to the signature with an <*authority*> tag. The <*authority*> element belongs to an XML namespace at "http://isec.gyte.edu.tr/rfcXX2.txt" with <*clearance*> and <*validity*> tags that meet the requirements of authorized signature structure are given as an example in Fig 3.

```
<Signature ID = "fooHierOrgSignature">
   <SignedInfo>
          ...
       <Reference URI= "#fooAuthority" TYPE=
       "http://www.w3.org/2000/09/xmldsig#SignatureProperties"
       >
   ...
       </SignedInfo>
         <Object>
           <SignatureProperties>
              <SignatureProperty ID = "fooAuthority"
           TARGET= "#fooHierOrgSignature"
                    <authority xmlns: myns=
                    "http:// isec.gyte.edu.tr foo.org.tr/rfcXX2.txt" >
                      <clearance > Level1</clearance >
                      <validity> 20071231</validity>
                    </authority>
                </SignatureProperty>
            </SignatureProperties>
         </Object>
</Signature>
```

Fig 3. The Authorized Signature Example Embedded To An XML Signature With <*SignatureProperties*> Element

A reference created and pointed to the Object element to provide the authorization must also be signed /approved. The <*authority*>, <*clearance*> and <*validity*> -a child element of <*date*>- must not be organization specific and can be standardized under the W3C standards.

V. SECURITY AND EFFICIENCY ANALYSIS OF THE PROPOSED HIERARCHICAL SIGNATURE SCHEME

We explored the existing electronic signature schemes in use to propose a scheme that also has backward compatibility with them. In this manner, we tried to ensure convenience of hierarchical organization in transition to our scheme.
We utilized the key efficiency of elliptic curve cryptography while designing the hierarchical signature scheme.
As in [14], the signature generation and verification phases of the proposed scheme is also based on gap Diffie Hellman groups and the security of the scheme is based on hardness of computational Diffie-Hellman problem. It is infeasible to compute a secret key from related public key in polynomial time.

The hash of authorization information is used in verification protocol to minimize the message size and as a prevention of man in the middle attacks that could use the authorization information.

In hierarchy, everybody would have a distinct electronic signature. If new signature keys were generated even each authorization changes in the hierarchical organization, everything would be worse than mentioned. The alteration of a managed key would response a chain reaction at all levels- entire key tree- if all levels have same level of verification authority. The proposed scheme generates the new signature as a union of the new extended authorization information and the already known and verifiable signature of the assigned person.

The scheme is flexible on selection of user's own secret key. The individuals generate their signature key according to their employed private-public key pair.

The key-derivation process is efficient. Derivation of hierarchical signature key requires hash and group computations only. Hierarchical signature key is derived with hash of authorization information and old signature key. Computation of a signature generation requires two hash function evaluation and some computations in G_1. The verification dominated with only a single pairing e computation.

The scheme has no exponentiation as in former id-based signature schemes [13, 14].

The proposed scheme manages the aforementioned authorization problems of hierarchical signature in case of assignment, promotion and new formation of authorities. The structure of authorization information is flexible for any hierarchical organization.

VI. Conclusions and Future Works

In this paper, we purposed a new hierarchical signature scheme. The new scheme is designed on the existing common schemes to satisfy backward compatibility and transition convenience.

Best of our knowledge, our scheme is the first hierarchical signature scheme that generates a signature key with association of authorization information and the signature key that is in circulation in a hierarchical organization.

It is common that person-specific unique identifiers like name, e-mail address- are used in signature generation as id-based signatures. Among signature schemes in literature, it is also a new approach to involve authorization information of an organization level in a signature generation.

This new structure -with the association of authorization information- ensures the continual usage of a known electronic signature even if its corresponding authorization is altered. This flexibility is helpful for key management of organizations.

We believe our hierarchical signature scheme could meet the future requirements of a hierarchical organization in terms of authorization. The verification clearance and boundaries of authorization information in the hierarchical structure are left as short-term future works.

References

[1] F.-G. Jeng, C-M. Wang: *"An efficient key-management scheme for hierarchical access control based on elliptic curve cryptosystem."* Journal of Systems and Software 79(8), 2006

[2]M. Mambo, K. Usuda, and E. Okamoto. "*Proxy signatures: Delegation of the power to sign messages"*. IEICE Trans. Fundamentals, 1996, Vol. E79-A, No. 9, pp. 1338-1353.

[3]G. Wang, F. Bao, J. Zhou, and R. H. Deng. *"Security Analysis of Some Proxy Signatures."* ICISC 2003, LNCS 2971, pp. 305-319. Springer-Verlag, 2004.

[4]G. Wang. "*Designated-Verifier Proxy Signature Schemes"*.IFIP/ SEC 2005, pp. 409-423. Springer, 2005.

[5] D. Chaum, H. V. Antwerpen, *"Undeniable Signatures",* CRYPTO '89 LNCS 435, Springer-Verlag, pp. 212-217.

[6] T.P. Pedersen. *"Distributed provers with applications to undeniable signatures"* Eurocrpt'91, LNCS 547, pp. 221-242. Springer-Verlag, 1991

[7]S. Saeednia, S. Kremer, O. Markowitch. *"An efficient strong designated verifier signature scheme"*, ICISC 2003, LNCS, pg 40-54, Korea, 2003.

[8]R. Steinfeld, L. Bull, H. Wang, J. Piperzyk, *"Universal Designated-Verifier Signatures"*,ASIACRYPT 2003, LNCS 2894, pp 523-542

[9] W. Ogata, K. Kurosawa, S-H Heng. *"The Security of the FDH Variant of Chaum's Undeniable Signature Scheme"*. PKC 2005, LNCS 3386, pp. 328-345. Springer-Verlag, 2005

[10]A. Shamir, *"Identity-Based Cryptosystems and Signature Schemes"*, CRYPTO 84, LNCS 7:47--53, 1984.

[11] D. Boneh, M. K. Franklin, *"Identity-Based Encryption from the Weil Pairing"*, Advances in Cryptology - Proceedings of CRYPTO 2001 (2001).

[12]Y. Zhou, Z. Cao, Z. Chai,"*Identity Based Key Insulated Signature"*, ISPEC 2006, LNCS 3903, pp. 226-234. Springer-Verlag, 2006

[13] K. G. Paterson, "*ID-based signatures from pairings on elliptic curves"*, IEEE Communications Letters, 38(18):1025–1026, 2002.

[14] J. C. Cha and J. H. Cheon, *"An identity-based signature from gap Diffie-Hellman groups"*, PKC 2003, LNCS vol. 2567 pag. 18-30. Springer-Verlag, 2003.

[15] C-Y Lin, T-C Wu, F.Zhang, J-J Hwang, *"New identity-based society oriented signature schemes from pairings on elliptic curves"*, Applied Mathematics and Computing 160, 2005

[16] XML-Signature WG, *http://www.w3.org/Signature/*, access. 2007

[17] J.Rosenberg, D.L. Remy, *Securing WebServices with WS-Security*, Sams Publ., 2004

[18] XML-Signature Syntax and Processing, *http://www.w3.org/TR/xmldsig-core/* , access. 2007