Proxy SmartCard

Giuseppe Cattaneo[1], Pompeo Faruolo[1], and Ivan Visconti[1]

Università di Salerno, Dipartimento di Informatica ed Applicazioni *R.M. Capocelli*,
Via Ponte don Melillo, I-84081 Fisciano (SA), Italy
{cattaneo,pomfar,visconti}@dia.unisa.it

Abstract. We present a ... bla bla

1 Introduction

The concepts of proxy signature and proxy cryptosystem was introduced respectively by Mambo et al.[1] in the 1996 and by Mambo and Okamoto[2] in 1997. In these schema an user, called *owner*, delegates another user, called *proxy user*, the power to execute own cryptographic tasks. In detail, the proxy user can sign messages on owner's behalf, in the proxy signature, and decrypt ciphertexts encrypted with owner's public key, in the proxy cryptosystem. In literature many extensions and improvements have been proposed for both schema, such as threshold proxy signatures[13], blind proxy signatures [15–17], proxy signatures with warrant recovery [xx], nominative proxy signatures [xx], one-time proxy signatures [18], and proxy-anonymous proxy signatures [6, 19–24]. Initially the schema was thought to be used in the large enterprise scenario, where a manager want delegate the sign of some documents in his absence or he can delegates his secretary to decrypt some emails encrypted using his public key. Successively these schema have been adopted in numerous other contexts such as, the electronics transaction [x], mobile agent environment [x] , distributed systems [x], grid computing [x], distributed shared object systems [x], global distribution networks [x], and mobile communications [x].
Most of these solutions are difficultly applicable in the real world, because they don't adopt the commonly used standard cryptography operations. For example, the verification of a delegate sign can not be accomplished by the conventional programs because it requires the custom verify. Moreover, these schema have the drawback of the impossibility to generate and store the private/secret keys on hardware tokens. Than the system that adopt them are vulnerability for the key handling and the users can not use own personal security hardware tokens.
Our contribute. We propose a system that allows the owner to delegate authorized users to sign messages on his behalf and decrypt ciphertexts encrypted with his public key through the use of his personal smartcard. The proxy users, after a strong authentication to the system, can access remotely to the owner's smartcard, sending a document to sing or a ciphertext to decrypted. If the request is compatible with the policies established by the owner for that proxy user, the system logs and executes the request forwarding the smartcard output.

The safety of smartcard is preserved because the proxy users can execute only sign and decrypt operations and these are performed only by the smartcard. Then the private and secret keys are never extract from the smartcard. We think that our system overcomes some drawbacks of the proxies schema. Indeed in our system there is a simple and efficient revocation mechanism, the complete knowledge by the owner of the signed messages and decrypted ciphertexts produced by the proxy users, the possibility to use the personal security tokens and the standard cryptographic operations.
Organization of the paper. In the Section 2 we review the proxy signature and cryptosystem schema proposed, in the Section 3 we present in detail our system....

2 Related work

In this section we report a state of art of the proxy signature and proxy cryptosystem schema, reporting their main characteristics.

2.1 Proxy Signature

...

In literature has been introduced by Mambo et al.[1] security requirements that a proxy signature schema should satisfy. Successively Lee et at. revisited them defining the following list of requirements today the commonly accepted.

Veriability : From a proxy signature, a verier can be convinced of the original signers agreement on the signed message

Strong unforgeability : Nobody, except the proxy user, cannot create a valid proxy signature

Strong Identiability : Anyone can determine the identity of the corresponding proxy user from a proxy signature.

Strong undeniability : A proxy signer cannot repudiate a proxy signature it created.

...

2.2 Proxy Cryptosystem

...

3 Proxy SmartCard System

The key of our system is to give to the proxy users the possibility to use the owners smart card without to compromise them and at the same time to maintain completely under control the proxy users activities. This is achieved allowing the remote access to some smart cards. The system is able to manage a set of smart

card reader connected to it, to which the users can access via web in order to accomplish sign and decrypt operations on the particular smart card. In our scenario, owners and proxy users have to registered them-self to our system. The owners put their smart cards into readers system and specify the proxy users, and with which features, can access to them. The proxy users, after logged in the system through a strong authorization mechanism, can use remotely the smart cards according to the policies established by the respectively owners. In detail, the owners can to authorize the delegation only for a time period and on a particular kind of documents, e.g. to decrypt only the email with a specified subject. Moreover, it possible to specify the kind of the proxy signature, that is, with or without warranty. In the former case, the signature will contain also a warning explaining that the signature is produced by a delegate. After to be authorized, the proxy users can submit to the system the requests. The proxy users must sign each requests with own private key, so that they cannot repudiate the requests. The system verified identity and the authorization of the proxy user, logs the request in order to allow the owners to check the activity of owns delegates. The owners can revoke the delegation to each proxy user in every time simply changing the policies of the user on the system. This withdrawal will have immediate effect, indeed, the revoked proxy user will not be able more to create a proxy signature. The past signature remain valid. We remark that our system respects all the security requirements introduced by Lee et al.[]. Indeed, the *Veriability* is satisfied because the signature is created with the private key of the owner. The *Strong undeniability* is achieved through the signature of the requests by the proxy users. The *Strong Identiability* and *Strong unforgeability* are satisfied in the warranty schema because the signature contain information about the signer created by himself with him private key and thus not forgery. Without the warranty schema all the additional information about the signer aren't linked to the signature but maintained on the system logs.

3.1 The Architecture

We implemented a prototype of our system in python language. It is composed by three main components, the the Dispatcher the RequestHandlers and the CardHandlers. The Dispatcher is a daemon in listening of the user requests and that dispatches them on the respective queue in waiting being executed. The RequestHandlers have access to these queues from which extract every time a new request that will be processed.

For each card reader there is a special process, the CardHandler, that is dedicate to handle in exclusive the reader. It invokes on its smart card the requests of a sign o decrypt and return the results to the RequestHandler.

References

1. M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures for delegating signing operation, in *ACM Conference on Computer and Communications Security*, pp. 48–57, 1996.

2. M. Mambo and E. Okamoto, Proxy cryptosystem: delegation of the power to decrypt ciphertexts, in *IEICE Trans. Fundamentals E80-A(1)*, pp. 54–63, 1997.
3. M.-S. Hwang, S.-F. Tzeng, and C.-T. Li, A new nonrepudiable threshold proxy signature scheme with valid delegation period, in *ICCSA (3)*, edited by O. Gervasi and M. L. Gavrilova, , Lecture Notes in Computer Science Vol. 4707, pp. 273–284, Springer, 2007.
4. H.-F. Huang and C.-C. Chang, Inf. Sci. **176**, 1338 (2006).
5. W. Liu, J. Yang, and L. Wei, A secure threshold proxy signature scheme for mobile agent-based electronic commerce transactions, in *PDCAT*, pp. 454–459, IEEE Computer Society, 2006.
6. Y. Yumin, A threshold proxy signature scheme with nonrepudiation and anonymity, in *ISCIS*, edited by A. Levi, E. Savas, H. Yenigün, S. Balcisoy, and Y. Saygin, , Lecture Notes in Computer Science Vol. 4263, pp. 1002–1010, Springer, 2006.
7. S. Lal and V. Verma, CoRR **abs/0806.1377** (2008).
8. P. yih Ting and X.-W. Huang, An rsa-based (t, n) threshold proxy signature scheme without any trusted combiner, in *ISC*, edited by T.-C. Wu, C.-L. Lei, V. Rijmen, and D.-T. Lee, , Lecture Notes in Computer Science Vol. 5222, pp. 277–284, Springer, 2008.
9. Z. L. Jiang, S.-M. Yiu, L. C. K. Hui, Y. Dong, and S. H. Y. Wong, Chained threshold proxy signature without and with supervision, In *CSSE (3)* [25], pp. 837–840.
10. F. Li, Q. Xue, and Z. Cao, Crypanalysis of kuo and chen's threshold proxy signature scheme based on the rsa, in *ITNG*, pp. 815–818, IEEE Computer Society, 2007.
11. J. Pomykala and S. Barabasz, Fundam. Inform. **69**, 411 (2006).
12. H. Bao, Z. Cao, and S. Wang, Identity-based threshold proxy signature scheme with known signers, in *TAMC*, pp. 538–546, 2006.
13. J. Shao, Z. Cao, and R. Lu, Journal of Systems and Software **80**, 172 (2007).
14. F. Kong, J. Yu, B. Qin, M. Li, and D. Li, Security analysis and improvement of a (t, n) threshold proxy signature scheme, in *SNPD (3)*, pp. 923–926, 2007.
15. W. Liu, F. Tong, Y. Luo, and F. Zhang, A proxy blind signature scheme based on elliptic curve with proxy revocation, in *SNPD (1)*, pp. 99–104, 2007.
16. Y. Qin and X. Wu, Cryptanalysis and improvement of two blind proxy signature schemes, In *CSSE (3)* [25], pp. 762–765.
17. Y.-S. Kim and J.-H. Chang, Provably secure proxy blind signature scheme, in *ISM*, pp. 998–1003, IEEE Computer Society, 2006.
18. R. Lu, Z. Cao, and X. Dong, Efficient id-based one-time proxy signature and its application in e-cheque, in *CANS*, edited by D. Pointcheval, Y. Mu, and K. Chen, , Lecture Notes in Computer Science Vol. 4301, pp. 153–167, Springer, 2006.
19. C. Hu and D. Li, A new type of proxy ring signature scheme with revocable anonymity, in *SNPD (1)*, pp. 866–868, 2007.
20. C. Hu, P. Liu, and D. Li, A new type of proxy ring signature scheme with revocable anonymity and no info leaked, in *MCAM*, pp. 262–266, 2007.
21. Z. Zhao, X. Tang, B. Li, and L. Zhu, An id-based anonymous proxy signature from bilinear pairings, in *Security and Management*, edited by H. R. Arabnia and S. Aissi, pp. 138–144, CSREA Press, 2006.
22. X. Zhou and P. Wei, Anonymous proxy authorization signature scheme with forward security, In *CSSE (3)* [25], pp. 872–875.
23. G. Fuchsbauer and D. Pointcheval, Anonymous proxy signatures, in *SCN*, pp. 201–217, 2008.

24. C. Fan, S. Zhou, and F. Li, Deniable proxy-anonymous signatures, in *ICYCS*, pp. 2131–2136, IEEE Computer Society, 2008.
25. *International Conference on Computer Science and Software Engineering, CSSE 2008, Volume 3: Grid Computing / Distributed and Parallel Computing / Information Security, December 12-14, 2008, Wuhan, China*, IEEE Computer Society, 2008.